

D-Link
Express EtherNetwork™
DSA-3100
Hotspot Gateway

Manual

January 2004
Fourth Edition

D-Link®

Building Networks for People

Contents

Package Contents	3
Introduction	4
Front Panel	5
Rear Panel	6
Features	7
Sample Scenarios	8
Installation	10
Setting Up the DSA-3100	11
Configure PCs on your LAN	12
TCP/IP Network Setting	12
Internet Access Configuration	13
Using the Configuration Utility	15
Networking Basics	55
Technical Specifications	68
Technical Support	70
Warranty and Registration	71

Package Contents



Contents of Package:

- 1** D-Link DSA-3100 Hotspot Gateway
- 2** CD-ROM (containing Manual and Warranty)
- 3** Quick Installation Guide
- 4** Two (2) CAT5 UTP/Straight-through (Ethernet) cables
- 5** One (1) CAT5 UTP/Cross-over cable
- 6** One (1) Console cable
- 7** 5V DC, 3A Power Adapter

If any of the above items are missing, please contact your reseller.

System Requirements for Configuration:

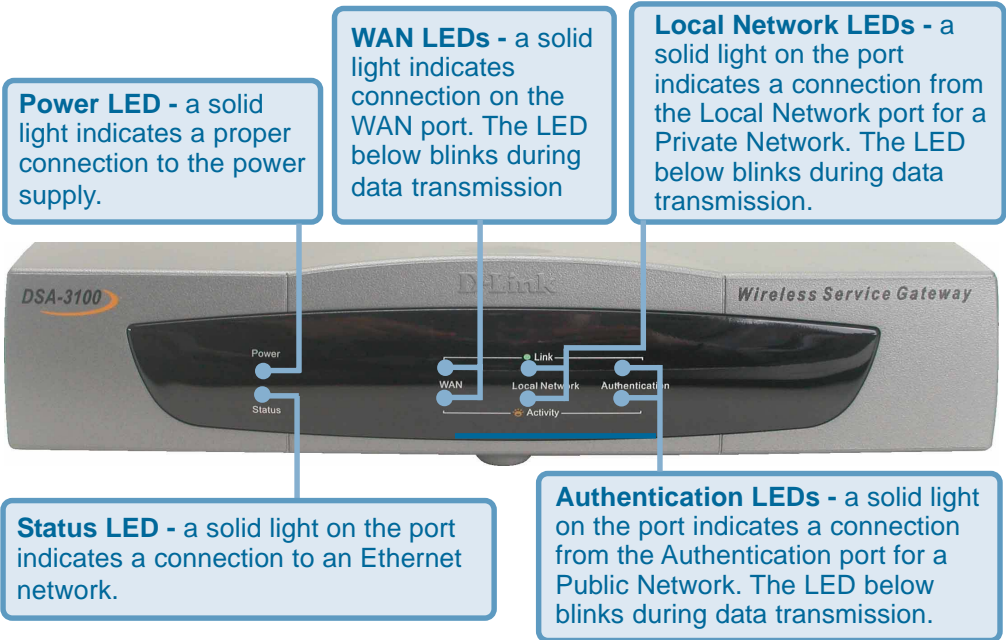
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator Version 6.0 and Above

Introduction

The D-Link DSA-3100 Hotspot Gateway is a simple-to-use network access control system supporting Ethernet, Fast Ethernet or an IEEE 802.11 wireless LAN (WLAN) separately and simultaneously.

The DSA-3100 can be configured with a standard HTML browser (i.e., Internet Explorer, Netscape Navigator) operating on Windows 98SE/Me/2000/XP, Macintosh OS 9, Mac OS X (v10.1.5 or later), Linux, or Pocket PC 2000/2002. The DSA-3100 allows the operator to offer wired or wireless networking services and access to the Internet when used with a switch or wireless access point respectively. The device features many management settings allowing for private and public access to the Internet and the necessary privilege mechanisms to permit this usage.

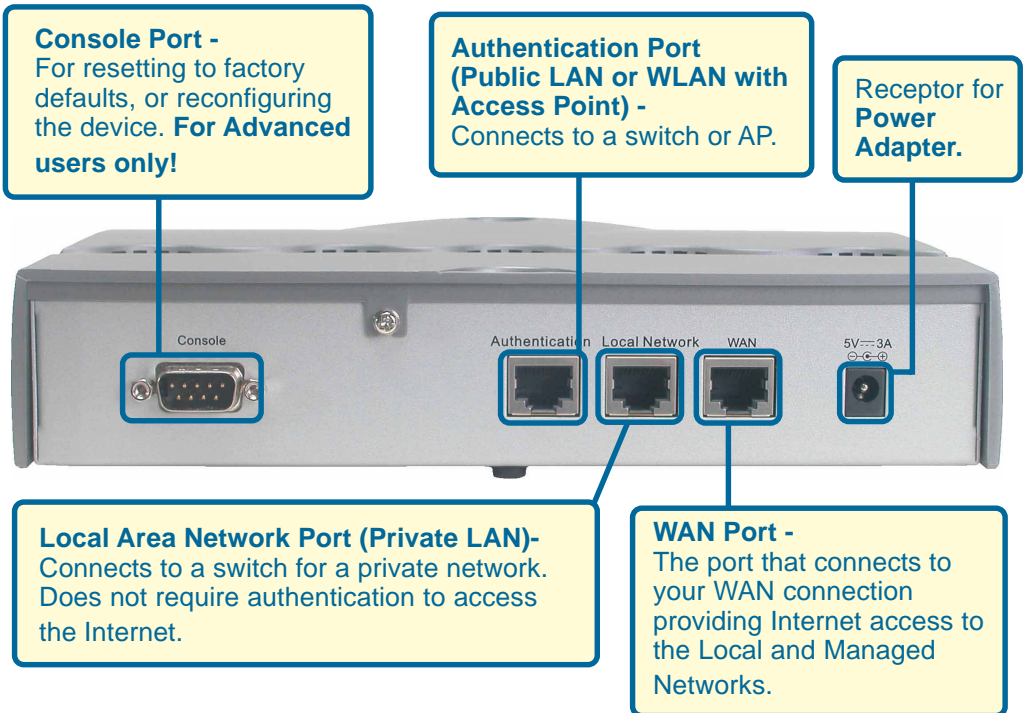
Front Panel



The Power Indicator remains illuminated when the DSA-3100 is on. The indicators for WAN, Local Network, Authentication each have two LED indicators. When CAT5 (Ethernet) cables are plugged into the corresponding port, the upper LED will illuminate to indicate that a connection has been established. The lower LED will blink whenever data is transmitted or received.

Power	Green LED		System is ready
Status	Green LED		System is ready
	Blinking LED		System is rebooting or Firmware upgrading
Link	WAN	Green	On line
	Local Network	Green	On line
	Authentication	Green	On line
Activity	WAN	Blinking	Data is being transmitted
	Local Network	Blinking	Data is being transmitted
	Authentication	Blinking	Data is being transmitted

Rear Panel

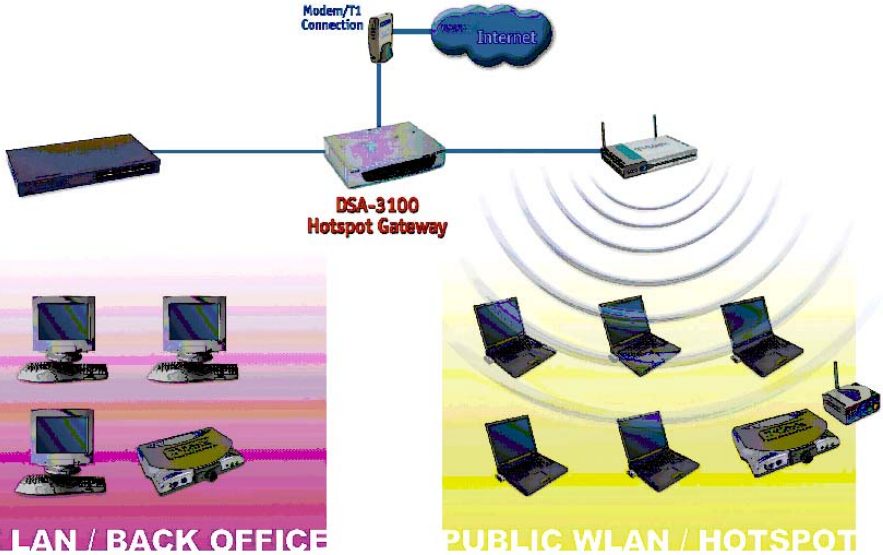


Features

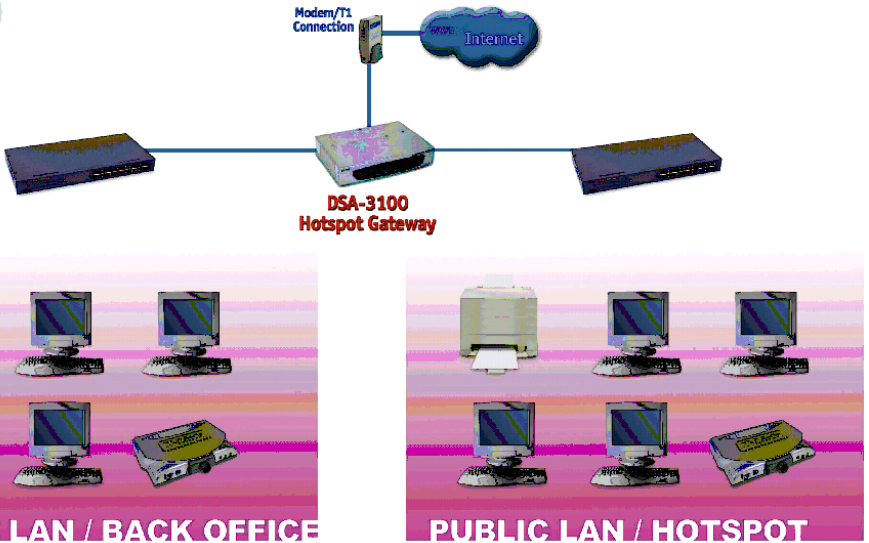
- Creates two separate and discreet networks allowing the owner/administrator to create a wired or wireless hotspot and provide Internet access to visitors, guests, or customers to your company or organization.
- Manages up to 250 user accounts with internal database.
- Supports at least 50 users accessing the Internet at any given time.
- Allows ID/Password-based authentication and authorization (can also be combined with MAC address locking for even stricter access control).
- Supports either POP3, RADIUS, or LDAP external authentication servers.
- Provides on-line status monitoring and historical traffic data.
- SSL-protected access to the administration interface and user authentication interface.
- Customizable user log-in and log-out Web interface.
- Customizable user log-out timer.
- Customizable target URL for users who successfully authenticate.
- Console mode administration interface via serial console port.
- Supports display of text messages on the log-in page. An administrator could use the administration interface to input messages (promotions, alerts, additional usage time/services with corresponding fees).
- Supports NAT for managed clients.
- Supports static IP, DHCP client and PPPoE client on the WAN interface.
- Built-in DHCP server to manage clients.
- Built-in, high-speed policy routing engine.
- Customizable peremptory traffic redirection (IP and Port-Redirect).
- Built-in NTP client.

Sample Scenarios

1

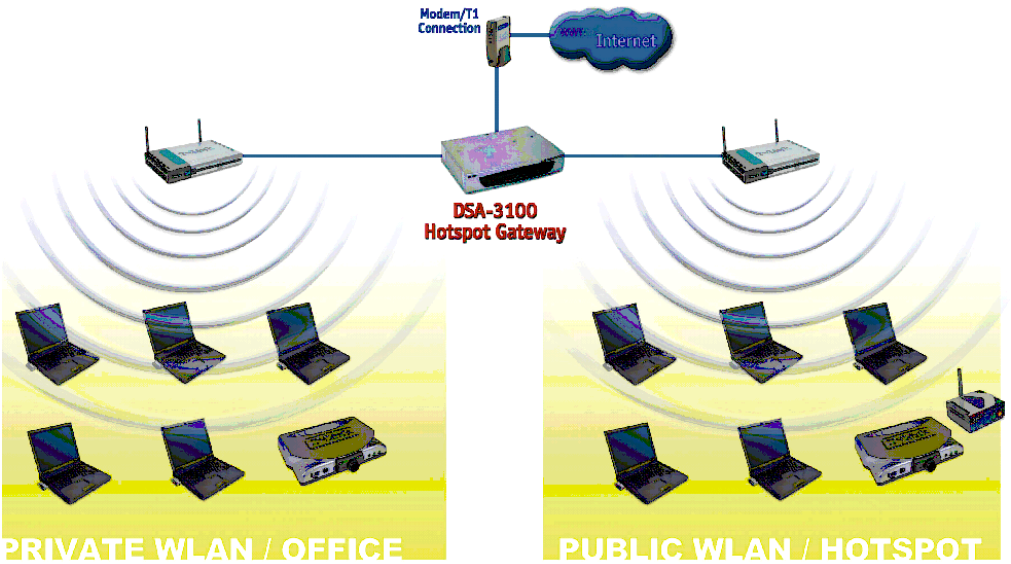


2



Sample Scenarios (continued)

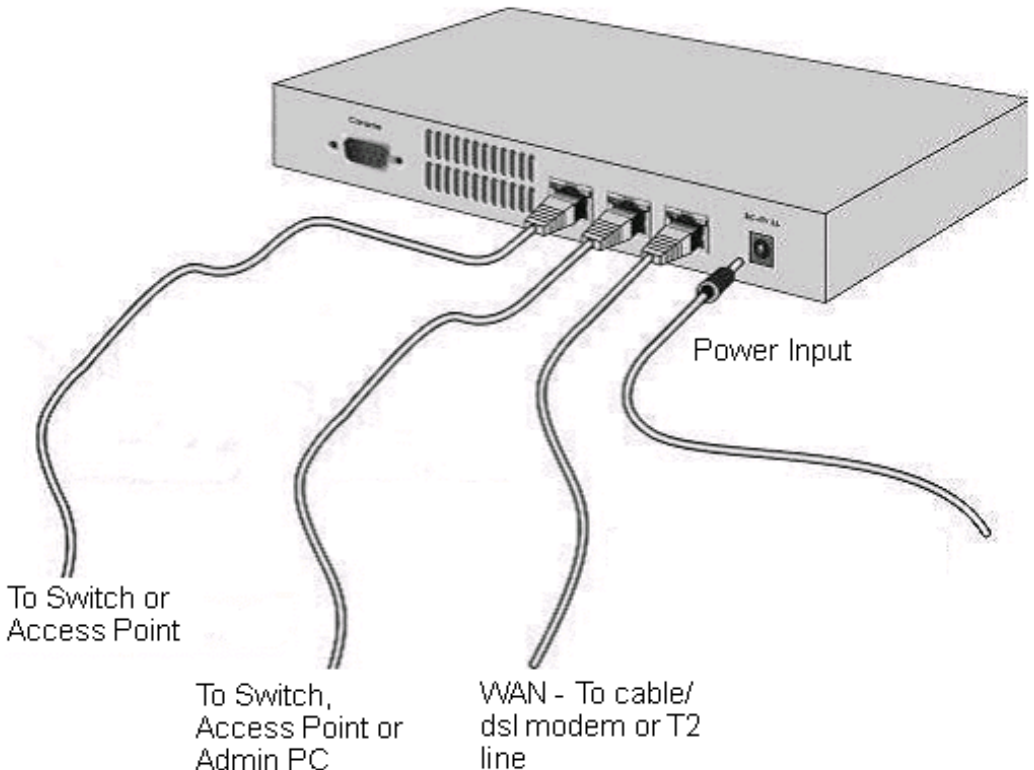
3



Installation

Requirements

- **Standard 10/100Base-T network (UTP/Cat5 Ethernet) cable with RJ45 connectors.**
- **TCP/IP network protocol must be installed on all networked computers and related devices.**



Setting up the DSA-3100

- **Make sure the DSA-3100 unit is not connected to the power adapter and is powered OFF.**

- **WAN port connection**

Use 10/100BaseT connections to connect the unmanaged network. The unmanaged network's interface may be the ADSL router's LAN port, cable modem's LAN port or Intranet switch port.

- **Private LAN port connection**

Use a straight-through cable to connect your admin PC with the internal switch or hub that is connected to the local network port on the DSA-3100. If you want to directly connect the DSA-3100 to this PC or the wireless AP, use a crossover cable.

- **Public LAN port connection**

Use a straight-through cable to connect your client PC with the internal switch or hub that is connected to the authentication port on DSA-3100. If you want to directly connect the DSA-3100 to this PC or the wireless AP, use a crossover cable.

- **Power ON**

Connect the supplied power adapter to the DSA-3100 and insert the plug on the other end into an electric outlet.

- **Check the LED**

The power LED and WAN LED should be ON, if the corresponding WAN port is connected to an active cable/DSL modem or T1 line.

- The corresponding local network or authentication indicator should be ON if a network device is connected to the local network port or the authentication internal port.

Configure PCs on your LAN

After installing the DSA-3100, each computer's **TCP/IP network setting** and **Internet** access configuration may need to be re-configured:

TCP/IP network setting

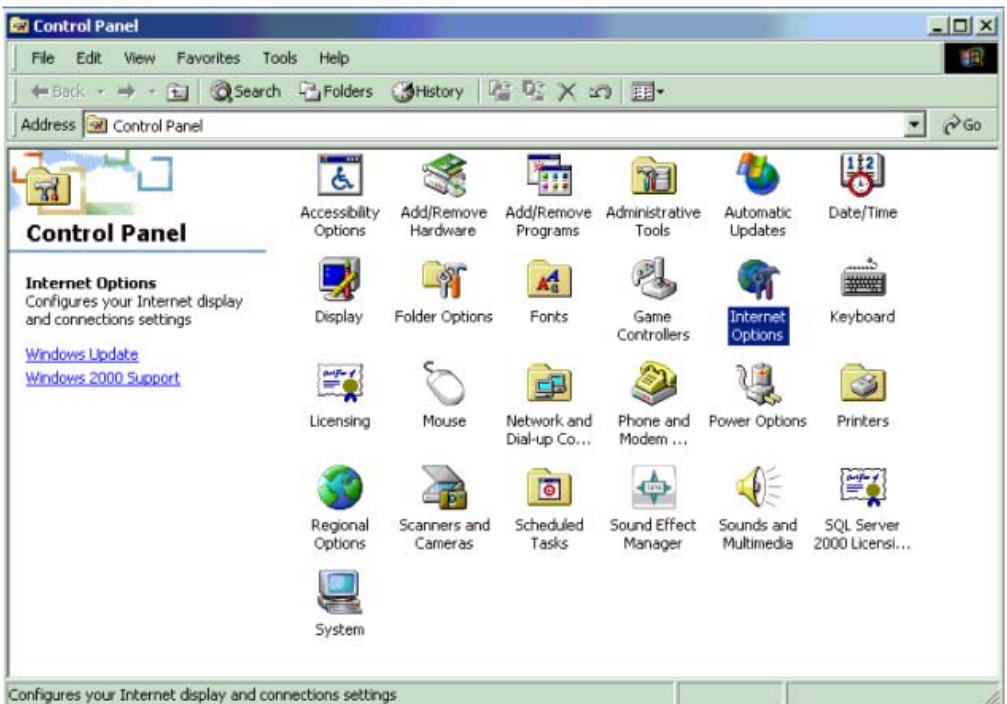
- If your PC uses the default Windows XP/2000/Me/98SE setting, no changes need to be made. Just start/restart your PC.
- If you are running Mac OS 9 or OS X, set your network settings to DHCP and select **Apply**.
- DSA-3100 will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each computer when the computer reboots or when the network settings refresh.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. In Windows, this is called *Obtain an IP address automatically*.
- If you are using a fixed IP address on your LAN, or if you want to check your TCP/IP setting, refer to the **Networking Basics** section in this manual.

Internet Access Configuration

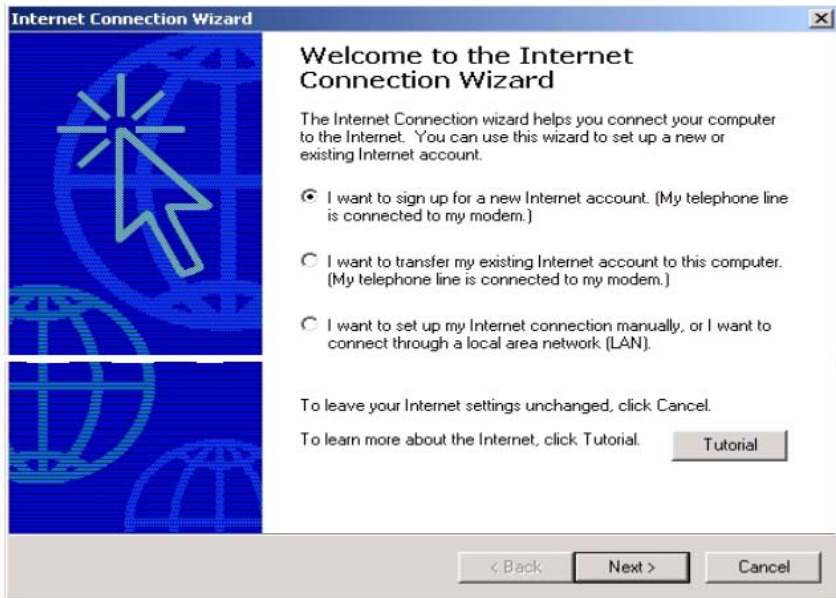
To configure your PCs to use the DSA-3100 for Internet access, follow this procedure.

For Windows 9x/2000

- Please select **Start Menu - Control Panel - Internet Options**.
- Select the Connection tab, and click the **Setup** button.
- Select “**I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)**” and click **next**.



Internet Access Configuration (continued)



- Select “**I connect through a local area network (LAN)**” and click **Next**.
- Ensure all of the boxes on the local area network Internet configuration screen are **unchecked**.
- Check **No**, when promoted “**Do you want to set up an Internet mail account now?**”
- Click **Finish** to close the Internet Connection Wizard. Setup is now completed.

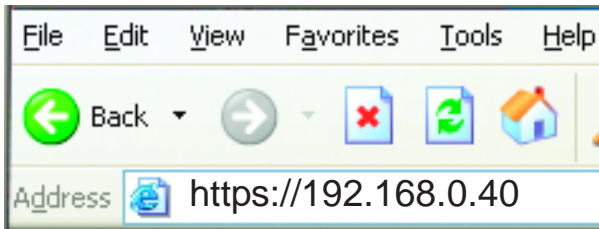
For Windows XP

- Please select **Star Menu - Control Panel - Network and Internet Connection**.
- Select the Connection tab, and click the **Setup** button.
- Click **Next** on the **New Connection Wizard** screen.
- Select **Connect to the Internet** and click **Next**.
- Select **Set up my connection manually** and click **Next**.
- Check **Connect using a broadband connection this always on** and click **Next**.
- Click **Finish** to close the New Connection Wizard. Setup is now completed.

Using the Configuration Utility

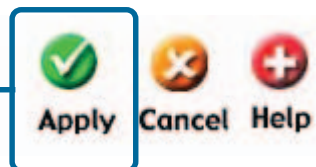
To configure the DSA-3100, use a computer which is connected to the local network port of the DSA-3100 with an Ethernet cable.

- First, disable the **Access the Internet using a proxy server** function. To disable this function, go to **Control Panel > Internet Options > Connections > LAN Settings** and uncheck the enable box.
- Start your Microsoft Internet Explorer Web browser program.
- Type the IP address of the DSA-3100 (the default IP address is 192.168.0.40) in the address field and press Enter. Make sure that the IP addresses of the DSA-3100 and your computer are in the same subnet.



On the bottom of each configuration screen you will find the buttons shown below.

Click **Apply** in each screen of the **Configuration Utility** in which you have made changes.



Restart the DSA-3100 after completing any changes to its configuration.

Using the Configuration Utility (continued)

Log-in Screen

You can log in as **admin** or as **manager**.

admin - the administrator of the DSA-3100.

User Name: admin

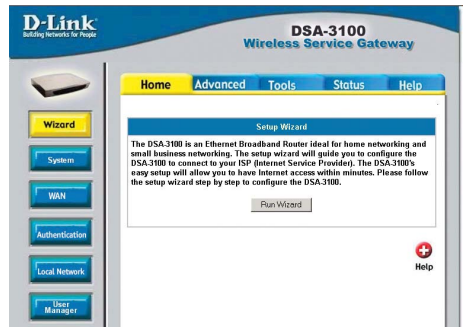
Password: admin

manager - access to the manager user account only.

User Name: manager

Password: manager

After you log in, click **Enter**.

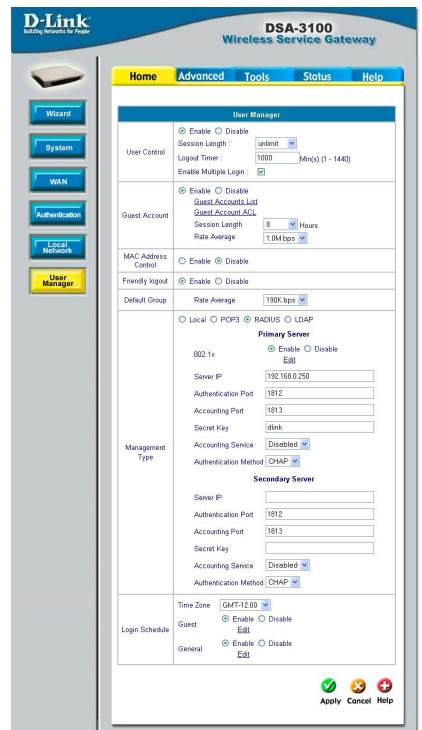


Home > Wizard

The **Home>Wizard** screen will appear if you logged in as an **admin**. For more information on the **Setup Wizard**, please see the *Quick Installation Guide*, included with your purchase. You can access the configuration features from this window.

Home > User Manager

The **Home>User Manager** screen will appear if you logged in as a **manager**. Please refer to the *Quick Installation Guide* for more information regarding the Setup Wizard. This screen will be explained in more detail in the following pages.



Using the Configuration Utility (continued)

System Name:

DSA-3100 is the default system name. You may wish to rename it to indicate your company, department, or the service you would like to provide.

Admin Detail:

You can edit the System Administrator's information here (e.g., name, phone number, and e-mail). If a user encounters a problem connecting to the WAN Port of the DSA-3100, the system administrator's information will be shown on the user login page

Succeed Page:

Enter a URL for all users to be directed to after successful login, typically defined as the home page of the host company, for instance: <http://www.dlink.com>. No matter to which URL a user originally attempts to connect, he/she will be directed to the URL defined here first.

SSH Manage IP:

Specify an IP address that connects to the WAN Port that will be allowed to configure the DSA-3100. For instance, if 10.2.3.1 is specified, then the user will be allowed to connect to the WAN Port and configure the DSA-3100 only from the specified address.

Access History IP:

Specify an IP address to be used by the billing system to connect to the DSA-3100 to get billing history information.

SNMP:

Simple Network Management Protocol is a system for managing complex networks. The DSA-3100 provides SNMP v2 Read-only(RO) management.

Manager IP: A trap manager is a management station that receives and processes traps. When you configure a trap manager, assign the IP address to the management station.

Community: Community strings serve as passwords for SNMP messages. DSA-3100 allows Read-only (RO) as a password.

If you **Enable** SNMP, enter the IP address and the community string in the field.

Home > System

The screenshot shows the D-Link configuration utility for the DSA-3100 Wireless Service Gateway. The 'System Configuration' page is active, displaying various settings. The 'System Name' is 'DSA3100'. The 'Succeed Page' is 'http://www.dlink.com'. The 'SSH Manage IP' is '102.3.1'. The 'Access History IP' is '192.168.2.1'. The 'SNMP' section has 'Enable' selected, 'Manager IP' set to '102.3.17', and 'Community' set to 'public'. The 'User login SSL' section has 'Enable' selected. The 'Time' section has 'NTP Server' set to 'ntp.usno.navy.mil', 'Time Zone' set to '(GMT+08:00)Taipei', and 'Set Device Date and Time' selected. The 'External Syslog Server' and 'Proxy Server' sections have empty fields. The 'History Email' and 'Admin Email' sections have 'Send from' and 'Send to' fields, and 'Interval' set to '1 Day'. The 'DNS Server' section has 'Preferred DNS Server' set to '168.95.1.1'. At the bottom right, there are 'Apply', 'Cancel', and 'Help' buttons.

continued -

Using the Configuration Utility (continued)

Home >System (continued)

User Logon

SSL: Select **Enable** or **Disable**

Time:

You may use **NTP** (Network Time Protocol) or you may input the time yourself. To use NTP please specify a timeserver's domain name and select the time zone. The time zone of the DSA-3100's internal clock is **UTC** (**C**oordinated **U**niversal **T**ime, formerly known as GMT, Greenwich Mean Time).

External Syslog Server:

Specify the IP address and the Port of the External Syslog server.

Proxy Server:

Specify the IP address and the Port of the Proxy server. (The DSA-3100 supports Http proxy).

History Email:

Send from: Indicate the IP address from which the email will be sent
Send to: Indicate the IP address to which the email will be sent
Interval: Indicate the interval at which the email will be sent

Admin Email:

Send from: Indicate the IP address from which the email will be sent
Send to: Indicate the IP address to which the email will be sent
Interval: Indicate the interval at which the email will be sent

DNS:

Specify DNS servers for the DSA-3100 for the Preferred DNS (preferred IP address) and Alternate DNS (alternate IP address).

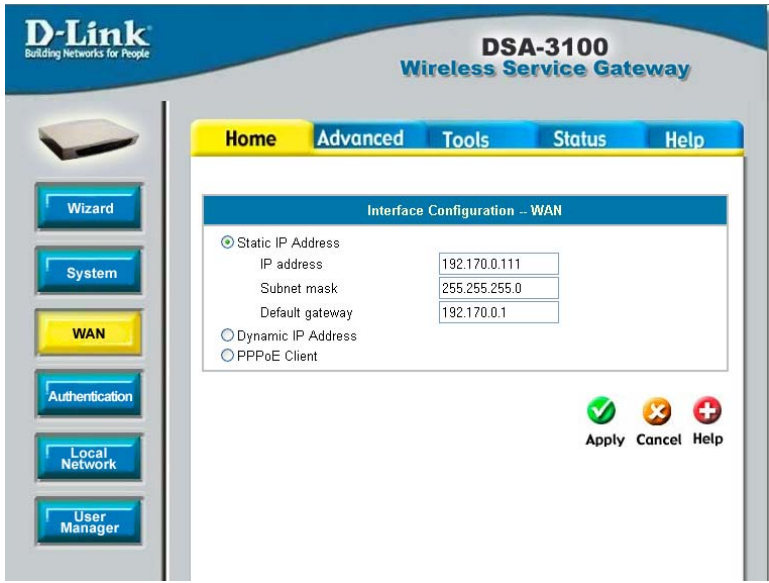
DoS protection for user:

The DSA-3100 protects users against various hacker attacks including:

- NMAP FIN/URG/PSH
- Xmas Tree
- SYN/RST,
- Ping of Death
- Null Scan
- SYN/FIN

Using the Configuration Utility (continued)

Home > WAN > Static IP Address



Static IP Address:

IP address: Enter the IP address provided to you by your ISP.

Subnet mask: Enter the subnetmask provided to you by your ISP. All devices on the network must share the same netmask.

Default Gateway: Enter the IP address of the gateway, provided to you by your ISP.

Dynamic IP Address: Make this selection if there is a DHCP server in the network. (See the following pages.)

PPPoE Client: Make this selection if you connect to the Internet using DSL. (See the following pages.)

Using the Configuration Utility (continued)

Home > WAN > Dynamic IP Address

The screenshot shows the configuration utility for a D-Link DSA-3100 Wireless Service Gateway. The interface is titled "Interface Configuration - WAN". On the left side, there is a navigation menu with buttons for "Wizard", "System", "WAN" (highlighted in yellow), "Authentication", "Local Network", and "User Manager". The main content area has tabs for "Home", "Advanced", "Tools", "Status", and "Help". Under the "Home" tab, the "Dynamic IP Address" radio button is selected, and a "Renew" button is visible next to it. Below the radio buttons are three icons: a green checkmark for "Apply", a red X for "Cancel", and a red plus sign for "Help".

Select this option to obtain an IP address automatically from your ISP.

Home > WAN > PPPoE

The screenshot shows the configuration utility for a D-Link DSA-3100 Wireless Service Gateway. The interface is titled "Interface Configuration - WAN". On the left side, there is a navigation menu with buttons for "Wizard", "System", "WAN" (highlighted in yellow), "Authentication", "Local Network", and "User Manager". The main content area has tabs for "Home", "Advanced", "Tools", "Status", and "Help". Under the "Home" tab, the "PPPoE Client" radio button is selected. Below it, there are input fields for "User Name" and "Password". There is also a "Maximum Idle Time" field with a "Minutes" label and a "Dial on demand" section with "Enable" and "Disable" radio buttons. At the bottom right, there are three icons: a green checkmark for "Apply", a red X for "Cancel", and a red plus sign for "Help".

User Name & Password:

Enter the user name and password that is assigned by your ISP.

Maximum Idle Time & Dial on demand:

These fields are optional.

Using the Configuration Utility (continued)

Home > Authentication

The screenshot shows the D-Link configuration utility for the DSA-3100 Wireless Service Gateway. The 'Authentication' tab is active. The 'Interface Configuration -- Authentication' section includes:
- Mode: NAT_IP_PNP (dropdown)
- IP Address: 192.168.1.40 (text field)
- Subnet Mask: 255.255.255.0 (text field)
The 'DHCP Configuration' section includes:
- Radio buttons for 'Disable DHCP Server' and 'Enable DHCP Server' (selected).
- DHCP Pool Start IP Address: 192.168.1.101 (text field)
- DHCP Pool End IP Address: 192.168.1.200 (text field)
- Lease Time: 1 Week (dropdown)
- Domain Name: dlink.com (text field)
- WINS IP Address: (empty text field)
- Preferred DNS Server: 192.152.81.1 (text field)
- Alternate DNS Server: 4.2.2.2 (text field)
- Radio button for 'Enable DHCP Relay' (unselected).
At the bottom right are 'Apply', 'Cancel', and 'Help' buttons.

The DSA-3100 allows the gateway to be set to one of three Authentication modes.

Mode: Select **NAT**; **NAT_IP_PNP** or **Router**

NAT: This mode protects the identity of the devices within the LAN from those devices outside the network.

NAT_IP_PNP: All devices, regardless of their IP address, can gain access to the Internet through the DSA-3100 in this mode.

Router: In this mode, the DSA-3100 will **not** protect the identity of the connected devices by translating their IP addresses and shielding them from detection outside the LAN.

IP Address: Enter the IP address for the Authentication interface (e.g., the RADIUS server in the network).

Subnet Mask: Enter the subnet mask for the Authentication interface

Disable DHCP Server: Make this selection if you do not wish to use the built-in DHCP feature in the DSA-3100

Using the Configuration Utility (continued)

Home > Authentication (continued)

Enable DHCP Server:

Selecting this option activates the device's built-in DHCP server. Configure the DHCP server with the following properties:

DHCP Pool Start IP Address: Enter the starting IP address, from which group of addresses the DHCP server will assign IP addresses to the DHCP-enabled devices (clients) on the network.

DHCP Pool End IP Address: Enter the last IP address in the sequence of addresses from which the DHCP server will assign addresses.

Lease Time: Select the length of time during which the DHCP assigned address will be in effect.

Domain Name: Enter the domain name.

WINS IP Address: Enter the WINS server's IP address.

Preferred DNS Server: Enter the IP address of the preferred DNS server.

Alternate DNS Server: Enter the IP address of the alternate DNS server.

Enable DHCP Relay:

Select this mode to specify another DHCP server's IP address.

Using the Configuration Utility (continued)

Home > Local Network

D-Link
Building Networks for People

DSA-3100
Wireless Service Gateway

Home Advanced Tools Status Help

Wizard
System
WAN
Authentication
Local Network
User Manager

Interface Configuration -- Local Network

Mode	NAT	
IP Address	192.168.0.40	
Subnet Mask	255.255.255.0	
DHCP Configuration	<input type="radio"/> Disable DHCP Server	
	<input checked="" type="radio"/> Enable DHCP Server	
	DHCP Pool Start IP Address	192.168.0.101 *
	DHCP Pool End IP Address	192.168.0.200 *
	Lease Time	1 Day
	Domain Name	dlink.com *
	WINS IP Address	
	Primary DNS IP Address	168.95.1.1 *
Secondary DNS IP Address		
	<input type="radio"/> Enable DHCP Relay	

Apply Cancel Help

NAT and **Router** are the two local network port modes.

Nat mode: All outbound IP addresses on the local network port will be translated to the IP address of the WAN port to proceed.

Router mode: All outbound IP addresses on the local network port will retain their IP addresses.

For an explanation of each field on this screen, please see the previous screen:

[Home > Authentication](#)

Using the Configuration Utility (continued)

Home > User Manager

The screenshot shows the configuration utility for a D-Link DSA-3100 Wireless Service Gateway. The page is titled "User Manager" and is part of the "Advanced" configuration section. The interface includes a navigation menu on the left with options like Wizard, System, WAN, Authentication, Local Network, and User Manager (which is highlighted). The main configuration area is divided into several sections:

- User Control:** Includes radio buttons for "Enable" (selected) and "Disable". Fields for "Session Length" (set to "unlimit"), "Logout Timer" (set to "10" Min(s)), and a checkbox for "Enable Multiple Login" (unchecked).
- Guest Account:** Includes radio buttons for "Enable" (selected) and "Disable". Links for "Guest Accounts List" and "Guest Account ACL". Fields for "Session Length" (set to "unlimit" Hours), "Logout Timer" (set to "10" Min(s)), and "Rate Average" (set to "unlimit").
- MAC Address Control:** Radio buttons for "Enable" and "Disable" (selected).
- Friendly logout:** Radio buttons for "Enable" and "Disable" (selected).
- Default Group:** "Rate Average" dropdown menu set to "unlimit".
- Management Type:** Radio buttons for "Local" (selected), "POP3", "RADIUS", "LDAP", and "External Server". Links for "Local Users List", "On-demand User Configuration", and "Local User Group Configuration".
- Login Schedule:** Radio buttons for "Guest" (selected) and "General", each with "Enable" and "Disable" options.

User Control: Select **Enable** to define **Logout Timer** and **Multiple Login**:

Session Length: Limit the duration of each session established by the general account from 5 minutes to an unlimited period.

Logout Timer: When enabled, on-line users who become inactive on the network after a specified period of time will be logged out automatically. The period can range from 1~1440. 10 minutes of time is the default value.

Multiple Login: Check this function to allow a single user account to log into the system multiple times.

Guest Account: Select **Enable** to activate the **Guest Account** feature for visitors

This close-up shows the "Guest Account" configuration section. It features radio buttons for "Enable" (selected) and "Disable". Below are links for "Guest Accounts List" and "Guest Account ACL". The "Session Length" is set to "unlimit" Hours. The "Logout Timer" is set to "10" Min(s). The "Rate Average" is set to "unlimit".

Using the Configuration Utility (continued)

Home > User Manager > Guest Accounts (continued)

Guest Account List:

Up to 10 guest accounts can be defined. To activate a particular **Guest Account**, simply enter the corresponding password in the **Password** column and click **Apply**.

No	User Name	Password
1	guest1	1234
2	guest2	
3	guest3	
4	guest4	
5	guest5	
6	guest6	
7	guest7	
8	guest8	
9	guest9	
10	guest10	

Guest Account ACL:

Define network areas where **Guest Account** is disallowed access, for instance 10.2.3.0/24.

Session Length:

You have the option to limit the duration for each session established by **Guest Account**, from 1~12 hours. There is no limit to the duration by default.

Logout Timer:

Logouts user if guest didn't access the Internet for a certain period.

Rate Average:

Limit the outbound traffic bandwidth for each session established by a Guest Account. There is no limit by default.

No.	Network ID	Subnet Mask
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

Using the Configuration Utility (continued)

Home > User Manager > MAC ACL Control

MAC Address Control	<input checked="" type="radio"/> Enable <input type="radio"/> Disable MAC ACL Control
---------------------	--

MAC Address Control:

When MAC address control is enabled, users connected to the Authentication Port can not login to the DSA-3100 unless they have registered their MAC Address at MAC Address Control. In other words, only 40 users will be allowed to login when this function is enabled. Please refer to the configuration screen as follows.

MAC ACL Control			
No.	MAC Address (XX:XX:XX:XX:XX:XX)	No.	MAC Address (XX:XX:XX:XX:XX:XX)
1	00:07:0E:B3:B0:09	2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	
21		22	
23		24	
25		26	
27		28	
29		30	


Note: MAC address format is **XX:XX:XX:XX:XX:XX** or **XX-XX-XX-XX-XX-XX**. A newly created user account will be valid instantly. Restarting the DSA-3100 is not necessary.

Using the Configuration Utility (continued)

Home > User Manager (continued)

Friendly logout:

If you enable Friendly logout, a pop-up window asking “Do you want to logout?” will appear after closing the login window. If you disable this function, no pop-up window will appear.

Friendly logout	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Default Group	Rate Average
	190K bps 
	<ul style="list-style-type: none">unlimit190K bps480K bps660K bps730K bps900K bps1.0M bps

Default Group:

Limit the outbound traffic bandwidth for On-demand users, RADIUS users, LDAP users, POP3 users to an average rate from 190Kbps-1Mbps.

Management Type:

Supports multiple user authentication methods including **Local**, **POP3 Server**, **RADIUS Server**, and **LDAP Server**.

Local:

User accounts are stored in the embedded database on the DSA-3100.

Management Type	<input checked="" type="radio"/> Local <input type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Server
	Local Users List On-demand User Configuration
	Local User Group Configuration

Local Users List: A list of all local user accounts stored in the embedded database for user account management. You can add, edit, and delete users. A sample list is shown here.

Local Users List			
User Name	MAC	Group	<input type="checkbox"/> Delete <input type="checkbox"/> Delete All
admin	00:80:c8:10:91:10	123	<input type="checkbox"/>
charlie	00:07:0e:b3:b0:09	345	<input type="checkbox"/>

(Total: 2) [First](#) [Prev](#) [Next](#) [Last](#)



Delete User: Click the box next to the user name and click **Delete**.

Add Users: Click **Add User** to create new accounts. The screen on the following page will appear.

Using the Configuration Utility (continued)

Home > User Manager > Management Type > Local > Local Users List

Add Users:

Add Users				
No	User Name	Password	MAC (12:34:56:78:90:12)	Group
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	group1
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	group1
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	group1
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	group1

Create new accounts, including **Username** (mandatory), **Password** (mandatory), and **MAC** (optional), and assign to a user group as shown above.

Edit Account:

Local Users List				
User Name	MAC	Group	<input type="button" value="Delete"/>	<input type="button" value="Delete All"/>
Lisa		group5	<input type="checkbox"/>	
Hans		group2	<input type="checkbox"/>	
Roson		group1	<input type="checkbox"/>	
Gavin		group3	<input type="checkbox"/>	

(Total:4) [First](#) [Prev](#) [Next](#) [Last](#)

Back

Make changes to the account by clicking on the User Name as indicated above. When the screen below appears, edit the account information.

Edit Account	
User Name	<input type="text" value="Lisa"/>
Password	<input type="text"/> <i>*Please leave the field blank, if you don't want to change password.</i>
MAC	<input type="text"/>
Group	group5

Back **Apply** **Cancel**


Using the Configuration Utility (continued)

Home > User Manager > Management Type > Local > Local Users List

Upload User Accounts:

Local Users List			
User Name	MAC	Group	Delete
Lisa		group5	<input type="checkbox"/>
Hans		group2	<input type="checkbox"/>
Roson		group1	<input type="checkbox"/>
Gavin		group3	<input type="checkbox"/>

(Total:4) [First](#) [Prev](#) [Next](#) [Last](#)



Besides adding user accounts one by one through the Web interface, you can prepare a text file, which contains user account information, store it on your hard drive and then upload it to the DSA-3100.

Each line of the text file can be in one of the following two formats:

UserID, Password, MAC
UserID, Password,

Please note that there must be no space or other characters between the user ID, password and the MAC address. The MAC address could be omitted, but the trailing comma must be retained. A user ID should be between 1 to 32 characters and the password should be between 0 to 20 characters. Special characters are not allowed for user name and password.

Upload User Account	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

After you have created the text file for the user account as described above, click **Upload User Accounts** as shown in the illustration at the top of this page. Click Browse and highlight the text file you have created.

Click **Refresh** for the latest information. Click **Apply** to update your changes.



Caution: When adding user accounts by uploading a file, existing accounts with the same **ID** will be replaced by the new ones.

Using the Configuration Utility (continued)

Home > User Manager > Management Type > Local > On-demand User Configuration

Management Type	<input checked="" type="radio"/> Local	<input type="radio"/> POP3	<input type="radio"/> RADIUS	<input type="radio"/> LDAP	<input type="radio"/> External Server
	Local Users List	On-demand User Configuration			
	Local User Group Configuration				

On-demand User: When you connect the DSA-3100P (the plug and play receipt printer) to the DSA-3100's console port, you can create a database of up to 2000 on-demand users. By default, the on-demand user database is empty. While you press the DSA-3100P's button, the on-demand user will be created in the database, a receipt will then be printed which will contain the on-demand user's information.

```

Welcome!
-----
Username: D-Link1
Password: q6m34m3b
Price: US$2
Usage: 60 minute(s)
-----
ESSID:
dlink
Shared WEP Keys
(HEX 40 bit):
1:
2:
3:
4:
-----
Valid to use until:
2003/09/09 12:46:56
-----
Thank You!
```

Shown above is an example of a an on-demand receipt.

Using the Configuration Utility (continued)

Home >User Manager >Management Type >Local >On-demand User Configuration (continued)

On-demand User Configuration	
Store name	D-Link (e.g.: D-Link. Max: 8 char)
Account range	from 0001 to 1000 (e.g.: 0001~2000. Max: 2000)
Receipt header	Welcome! (e.g.: Welcome!)
Receipt footer	Thank You! (e.g.: Thank You!)
Printer baud rate	9600
Account expires after	3 days
Session expires after	60 minutes
Logout timer	10 Min(s) (1 - 1440)
WLAN ESSID	dlink (e.g.: dlink)
WEP key	1: <input type="text"/>
WEP key	2: <input type="text"/>
WEP key	3: <input type="text"/>
WEP key	4: <input type="text"/>
Price	US\$2 (e.g.: US\$2)

Field	Description
Store Name	You can specify the prefix of the user name. The maximum is 8 characters (e.g., D-Link).
Account Range	You can specify the maximum user amount which cannot exceed 2000.
Receipt Header	You can configure the receipt's header in this field.
Receipt Footer	You can configure the receipt's footer in this field.
Printer baud rate	You can specify the baud rate to support a specific printer. The default setting is 9600.
Account expires after __ days	You can specify the days before expiration in this field. After the expiration date the user account will no longer be available. A new session will be required.
Session expire after __ minutes	You can specify how many minutes this account will be available after successful login.
Logout timer	Logout user if the guest didn't access the Internet for a certain period.
WLAN ESSID	You can specify the access point's ESSID in this field.
WEP Key	You can specify the access point's WEP key in the WEP key field.
Price	You can specify the price in this field.

Using the Configuration Utility (continued)

Home > User Manager > Management Type > Local > On-demand User Configuration (continued)

User List

On-demand Users List					
User Name	Password	Expiration Date	Session Length	Status	
					Delete
					Delete All

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#)

Click **User List** in the previous screen and the screen above will appear showing a list of the on-demand users. You can delete users in this window.



Back

Local > Local User Group Configuration

Management Type	<input checked="" type="radio"/> Local	<input type="radio"/> POP3	<input type="radio"/> RADIUS	<input type="radio"/> LDAP	<input type="radio"/> External Server
	Local Users List On-demand User Configuration				
	Local User Group Configuration				

The DSA-3100 provides 5 local user groups; each group can designate a different outbound traffic bandwidth. The Logout Timer will logout a user that has not accessed the Internet for a certain time period. A sample list is shown below.

Local User Group Configuration			
No	Group Name	Logout Timer Min(s) (1 - 1440)	Rate Average
1	<input type="text" value="group1"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/>
2	<input type="text" value="group2"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/>
3	<input type="text" value="group3"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/>
4	<input type="text" value="group4"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/>
5	<input type="text" value="group5"/>	<input type="text" value="10"/>	<input type="text" value="unlimited"/>

Using the Configuration Utility (continued)

Home > User Manager > Management Type > POP3

Management Type	<input type="radio"/> Local <input checked="" type="radio"/> POP3 <input type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Server
	Server IP <input type="text"/>
	Server Port <input type="text" value="110"/>

To use POP3 as the authentication method, input the **POP3** server IP address or domain name and its POP3 server port. The settings will take effect immediately after you click the **Apply** button. It is recommended that you restart the DSA-3100 after these changes if there are any online users.

Home > User Manager > Management Type > RADIUS

Management Type	<input type="radio"/> Local <input type="radio"/> POP3 <input checked="" type="radio"/> RADIUS <input type="radio"/> LDAP <input type="radio"/> External Server
	Session/Idle <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Primary Server
	802.1x <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Server IP <input type="text"/>
	Public LAN Port <input type="text" value="1812"/>
	Accounting Port <input type="text" value="1813"/>
	Secret Key <input type="text"/>
	Accounting Service <input type="text" value="Disabled"/>
	Public LAN Method <input type="text" value="CHAP"/>
	Secondary Server
	Server IP <input type="text"/>
	Public LAN Port <input type="text" value="1812"/>
	Accounting Port <input type="text" value="1813"/>
Secret Key <input type="text"/>	
Accounting Service <input type="text" value="Disabled"/>	
Public LAN Method <input type="text" value="CHAP"/>	

To use RADIUS as the authentication method, input the RADIUS server IP address or domain name, public LAN port, accounting Port, secret key and select the accounting service and public LAN method function. The settings will take effect immediately after you click the **Apply** button. It is recommended that you restart the DSA-3100 after these changes if there are any online users.

Using the Configuration Utility (continued)

Home > User Manager > Management Type > RADIUS > 802.1x

Select **Enable** to use the 802.1x feature. The DSA-3100 supports integrated single sign-on when using with 802.1x enabled access points. By using the integrated RADIUS proxy function in the DSA-3100, users can use the EAP methods such as EAP-MD5 or EAP-TLS to login and get the service depending on the authentication methods which the backend RADIUS server and APs support.

The assumption, for this scenario, is that the network administrator had configured an EAP-enabled RADIUS server like Microsoft Internet Authentication Service on Windows 2000 or .NET Server 2003. If EAP-TLS is required for the dynamic key exchange, Microsoft Certification is also required. It is also recommended that the system administrator perform an authentication test to make sure everything is correct before connecting the network to the DSA-3100. (802.1x is available only when RADIUS is selected here, under *Management Type* in the DSA-3100 Configuration).

To utilize 802.1x, all the devices on the network must be 802.1x and EAP enabled. The APs and the RADIUS server must share the same secret word; and the DSA-3100 and the RADIUS server must share the same secret word.

Configuring network devices for use with 802.1x:

To use 802.1x, please configure the RADIUS server, the access points and the DSA-3100 as follows :

RADIUS server:

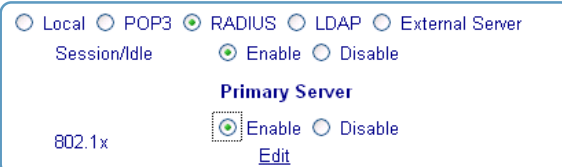
The system administrator should create a client account for the DSA-3100 first and define the required secret. (We suggest that you use a different one than the one the APs are using). The RADIUS server is capable of multiple "secret keys" each assigned to a specific device. In order to participate in the network, each device must share the secret key that has been assigned to it in the RADIUS server's configuration.

DSA-3100:

In the configuration utility, select Home>User Manager>Management Type and select RADIUS.

Access Points:

When configuring the access point, include the IP address of the RADIUS server in the appropriate field. The corresponding secrets for each AP should match the settings in DSA-3100. Click **Edit** (as shown below) to input the **IP addresses** and the **secret keys** of the access points in your network.



The screenshot shows a configuration window with the following elements:

- Radio buttons for server type: Local, POP3, **RADIUS** (selected), LDAP, External Server.
- Radio buttons for status: **Enable** (selected), Disable.
- Section header: **Primary Server**
- Radio buttons for 802.1x status: **Enable** (selected), Disable.
- An **Edit** button located below the 802.1x status options.

Using the Configuration Utility (continued)

Home > User Manager > Management Type > RADIUS > 802.1x (continued)

Input the IP addresses and secret keys for the devices on the network.

802.1x Device Configuration		
No	IP (Segment) Address	Secret
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>



If you are using the 802.1x supplicant provided by Microsoft, the idle time out will be longer than the settings in RADIUS/AP and DSA-3100. Except for the idle timer, there is no way for the user to logoff from 802.1x Access Point in the current 802.1x implementation by Microsoft.

Using the Configuration Utility (continued)

Home > User Manager > Management Type > LDAP

LDAP:

Management Type	<input type="radio"/> Local	<input type="radio"/> POP3	<input type="radio"/> RADIUS	<input checked="" type="radio"/> LDAP	<input type="radio"/> External Server
	Server IP	<input type="text"/>			
	Server Port	<input type="text" value="389"/>			
	Base DN	<input type="text" value="CN=Users,DC=dlink,DC=com"/>			

To use LDAP as the authentication method, input the LDAP server IP address or domain name and its LDAP server port. The settings will take effect immediately after you click the **Apply** button. It is recommended that you restart the DSA-3100 after these changes if there are any online users.

Login Schedule:

Define the time zone where the DSA-3100 is located and login duration for **Guest** and **General accounts**. By default the time zone is GMT-07:00.

Login Schedule	Guest	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
		Edit	
	General	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Define login duration for Guest accounts. Select **Enable - Edit** to enter the management interface (as shown above). After durations are defined, you need to click **Apply**, and then **Save All** to let the new functions take effect.

To define the login duration for General accounts use the same procedure as above.

Login Schedule -- Guest							
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Using the Configuration Utility (continued)

Advanced > Port and IP Redirect



The screenshot shows the configuration utility for a D-Link DSA-3100 Wireless Service Gateway. The interface is in the 'Advanced' tab, specifically the 'Port and IP Redirect' section. On the left, there is a sidebar with navigation buttons: 'Port and IP Redirect' (highlighted), 'Pass Through', 'Virtual Server', 'DMZ', 'Free Surfing Area', 'Static Route', and 'Firewall'. The main area contains a table for defining redirection rules, with columns for 'Destination' (IP Address and Port) and 'Convert to Destination' (IP Address and Port). The 'Type' column has radio buttons for 'TCP' and 'UDP'. Below the table are 'Apply', 'Cancel', and 'Help' buttons.

No.	Destination		Convert to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP

Apply Cancel Help

Up to 10 sets of traffic redirection criteria could be defined through this interface. Clients who try to access a specific destination that matches one of the defined destinations will be forced to a matching redirection target. These settings will take effect immediately after you click the **Apply** button.

Using the Configuration Utility (continued)

Advanced > Pass-Through

To maintain an adequate level of security, each client on the network can be managed. To allow some devices to be unmanaged, input their IP addresses or MAC addresses in this interface. Up to 20 IP addresses and 10 MAC addresses can be assigned unmanaged access. MAC address format is XX:XX:XX:XX:XX:XX

Pass through IP & MAC Configuration			
No.	IP Address	No.	IP Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

No.	MAC Address	No.	MAC Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>



Caution: Allowing unmanaged access from specific IP or MAC addresses could adversely affect the security of your network.

This feature allows you to define up to 10 virtual servers to enable access to servers connected to the authentication and local network port from outside of the managed network. Depending on the service provided, the service might run on TCP ports, UDP ports or both. Click **Enable** to activate the rule. Changes to the settings of virtual servers will take effect immediately after you click the **Apply** button.

Advanced > Virtual Server

Virtual Server Table						
No.	External Service Port	Local Server IP Address	Local Service Port	Type	Enable	
1	21	192.168.1.80	21	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
2	1723	192.168.0.250	1723	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
3	500	192.168.0.250	500	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>	

Apply Cancel Help

Note: Each local server connected to the authentication port must also be allowed IP or MAC address pass-through. Please enter its IP or MAC address via the interface shown in the pass-through configuration screen.

Using the Configuration Utility (continued)

Advanced > DMZ

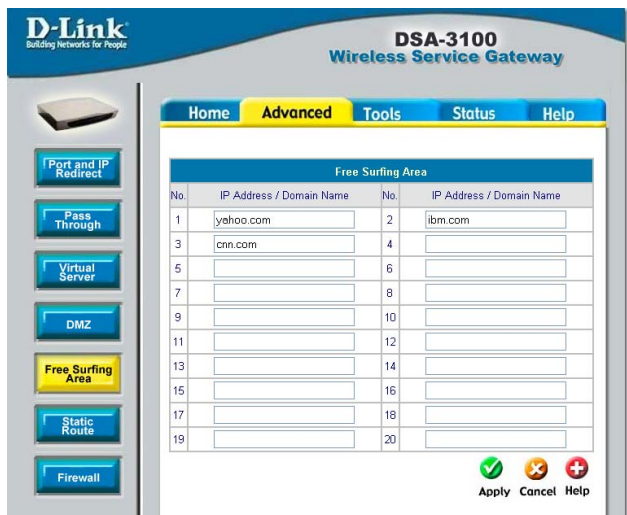
If you have multiple IP addresses available to assign to the DSA-3100's WAN interface, you could define up to 10 pairs of Ethernet side (Private IP) and WAN side (Public IP) addresses. The WAN interface will bind the extra public IP addresses automatically.



No.	Private IP Address	Public IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

To allow users access to a few websites before they log in, enter the IP addresses of those sites in the **Free Surfing Area** list. Up to 10 sites can be defined. For example, a website that provides introduction and guidance for local facilities and routes or sites with content suitable or appropriate for public viewing could be listed in the **Free Surfing Area**. Guest users of the network cannot access other parts of the network but could still connect to these sites.

Advanced > Free Surfing Area



No.	IP Address / Domain Name	No.	IP Address / Domain Name
1	yehoo.com	2	ibm.com
3	cnn.com	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

These sites provide a free experience but can also indicate other areas of the Internet that can be accessed for an additional fee.

Using the Configuration Utility (continued)

Advanced > Static Route

In this example, if you want the 192.168.202.0/24 and 192.168.100.0/24 network to have access to each other, you should add a static route in the DSA-3100 and also in the 192.168.200.253 IP router. The following settings show the DSA-3100's static route configurations.

The screenshot shows the D-Link DSA-3100 configuration utility. The 'Advanced' tab is active, and the 'Static Route' configuration page is displayed. The page features a table with 10 rows for configuring static routes. The first row is pre-filled with the following values:

No.	Destination		Gateway
	Network ID	Subnet Mask	IP Address
1	192.168.202.0	255.255.255.0	192.168.0.253
2			
3			
4			
5			
6			
7			
8			
9			
10			

At the bottom right of the configuration page, there are three buttons: 'Apply' (with a green checkmark), 'Cancel' (with a red X), and 'Help' (with a red plus sign).

Destination Network ID:

Specifies the target network or host IP. In this example we use network 192.168.202.0 as the routed target.

Destination Subnet Mask:

Specifies the target subnet mask. In the example, we use the subnet mask 255.255.255.0.

Gateway IP Address:

Specifies the IP address of the next hop router. In the example, we set this to 192.168.0.253 as the 192.168.202.0 network is behind the router.

Click Apply:

Always click **Apply** to save the changes/additions.

Note: For the static route to work, the next hop route must also have added a static route to forward all 192.168.100.0/24 IP packets to the DSA-3100. After clicking the **Apply** button, you will see the added route is shown in the current running routing table. Click “ **View Routing table** ” to verify.



Every change to the static route settings must be stored by using the *Save Setting* function, and restarting the DSA-3100.

Using the Configuration Utility (continued)

Advanced > Firewall

Click the **Filter Rule** number to enter the firewall page for each filter. The chart on the following page explains each configurable item in detail.

D-Link
Building Networks for People

DSA-3100
Wireless Service Gateway

Home **Advanced** Tools Status Help

IP Filter / Firewall

Filter Rule	Active	Action	Name	Source	Destination	Protocol
1	<input checked="" type="checkbox"/>	Block	AU-LN Disallow	ANY	ANY	ALL
2	<input type="checkbox"/>	Block		ANY	ANY	ALL
3	<input type="checkbox"/>	Block		ANY	ANY	ALL
4	<input type="checkbox"/>	Block		ANY	ANY	ALL
5	<input type="checkbox"/>	Block		ANY	ANY	ALL
6	<input type="checkbox"/>	Block		ANY	ANY	ALL
7	<input type="checkbox"/>	Block		ANY	ANY	ALL
8	<input type="checkbox"/>	Block		ANY	ANY	ALL
9	<input type="checkbox"/>	Block		ANY	ANY	ALL
10	<input type="checkbox"/>	Block		ANY	ANY	ALL

First Prev Next Last

Apply Cancel Help

Edit the filter rule

Filter rule is a set of filters that determine whether traffic will be allowed to pass between the source and destination or whether it will be dropped. To display the detail, click the **index number** in the screen above.

IP Filter / Firewall > Edit Filter Rule

Rule: 1

Name: Check to enable this rule

Action: Protocol:

Source MAC:

	IF	Address	Subnet Mask	Operator	Start Port	End Port
Source	<input type="text" value="AU"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>
Destination	<input type="text" value="LN"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input "="" type="text" value="="/>	<input type="text"/>	<input type="text"/>

On the following page please find an explanation of the fields in the above configuration screen.

Using the Configuration Utility (continued)

Advanced > Firewall (continued)

Filter	Description
Name	To give a name to an IP Filter rule
Check to enable this rule	Enable this rule if it is marked
Action	Specifies the action to be taken when packets match the rule Block: Packets matching the rule will be dropped immediately Pass: Packets matching the rule will be passed immediately
Protocol	Specifies the protocol(s) this filter rule will apply to
Source MAC	Source MAC address
Source/ Destination IF	Source/Destination Interface. You can select WAN port or LAN port or Authentication port or ALL ports
Source/ Destination IP Address	Source/Destination IP Address
Source/Destination Subnet Mask	Source/Destination Subnet Mask
Source/Destination Operator	Select =(equal), != (not equal), >(greater than), <(smaller than) operator rule
Source/Destination Start Port	Source/Destination Start Port
Source/Destination End Port	Source/Destination End Port

Using the Configuration Utility (continued)

DSA-3100 can monitor the IP address from anywhere; up to 20 IP addresses can be monitored. The system periodically sends out packets to check the status of the selected network nodes by pinging every 30 minutes. If the node cannot be reached, the DSA-3100 will send an E-mail to the admin. every 30 minutes. For example: if you specify a node which can't be reached, the DSA-3100 will send an E-mail to the admin. at 1:00, 1:30, 2:00, 2:30, 3:00..etc, until the problem is fixed.

Tools > Monitor IP List

The screenshot shows the 'Monitor IP List' configuration page. The table below is a representation of the data shown in the interface:

No.	IP Address	No.	IP Address
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

DSA-3100 provides 2 built-in user accounts: **Admin** and **Manager**

Admin: This user is the administrator of the DSA-3100.

Manager: This user has the right to manage a user account, the admin. functions are denied.

The Admin and the Manager can change their passwords; specify the current password first. The new password must be entered twice.

Tools > Change Password

The screenshot shows the 'Change Password' configuration page. It contains two forms for changing passwords:

Change Admin Password

Old Password	<input type="text"/>
New Password	<input type="text"/>
New Password (confirm)	<input type="text"/>

Change Manager Password

Old Password	<input type="text"/>
New Password	<input type="text"/>
New Password (confirm)	<input type="text"/>



Note: If you lose the administrator's password, you can change the administrator's password from the console interface.

Using the Configuration Utility (continued)

Tools > Upload customer Key



Upload customer KEY

File Name Browse...

Use Default KEY Apply Cancel Help

To provide a custom key page in order to support a specific certificate, please click **Browse** to search for the file name for the customer key. Click **Apply** to upload it onto the DSA-3100. If you want to get back to the default customer Key page, simply click the **Use Default KEY** button.

Tools > Upload customer certificate



Upload customer certificate

File Name Browse...

Use Default CA Apply Cancel Help

To provide a custom key page in order to support a specific certificate, please click **Browse** to search for the file name for the customer certificate. Click **Apply** to upload it onto the DSA-3100. If you want to get back to the default customer certificate page, simply click the **Use Default CA** button.

Using the Configuration Utility (continued)

Tools > Upload Login Page



The screenshot shows a web-based configuration utility titled "Upload Login Page". It features a "File Name" input field with a "Browse..." button to its right. Below the input field are three buttons: "Preview", "Use Default Page", and "Apply". To the right of the "Apply" button are three icons: a green checkmark, an orange 'X', and a red plus sign, with the labels "Apply", "Cancel", and "Help" respectively.

To provide a custom user login page, please specify the file name to upload onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Login page, simply click the **Preview** button

The uploaded custom login page must contain the following HTML codes to provide users a place to input the user name and password.

Required HTML code

```
<form action="userlogin.shtml" method="post" name="Enter">  
<input type="text" name="myusername">  
<input type="password" name="mypassword">  
<input type="submit" name="submit" value="Enter">  
<input type="reset" name="clear" value="Clear">  
</form>
```

Using the Configuration Utility (continued)

Tools > Upload Logout Page

Upload Logout Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
Preview	<input type="button" value="Use Default Page"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>

To provide a custom user logout page, please click **Browse** to specify the file name and upload it onto the DSA-3100 by clicking **Apply**. If you want to get back to the default user logout page, simply click the **Use Default Page** button. If you want to display the Logout page, simply click the **Preview** button.

The uploaded custom logout page must contain the following HTML codes to provide users a place to input the user name and password.

Required HTML code

```
<form action="userlogout.shtml" method="post" name="Enter">  
<input type="text" name="myusername">  
<input type="password" name="mypassword">  
<input type="submit" name="submit" value="Logout">  
<input type="reset" name="clear" value="Clear">  
</form>
```

Using the Configuration Utility (continued)

Tools > Upload Login error Page

Upload Login error Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
Preview	<input type="button" value="Use Default Page"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
	Apply Cancel Help

Upload Login error Page: To provide a custom user login error page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Login error Page, simply click the **Preview** button.

Tools > Upload Login Succeed Page

Upload Login Succeed Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
Preview	<input type="button" value="Use Default Page"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
	Apply Cancel Help

Upload Login Succeed Page: To provide a custom user "login ok" page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Login Succeed Page, simply click the **Preview** button.

Tools > Upload Logout Succeed Page

Upload Logout Succeed Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
Preview	<input type="button" value="Use Default Page"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
	Apply Cancel Help

Upload Logout Succeed Page: To provide a custom user logout page, please specify the file name to upload it onto the DSA-3100. If you want to get back to the default user login page, simply click the **Use Default Page** button. If you want to display the Logout Succeed Page, simply click the **Preview** button.

Using the Configuration Utility (continued)

Tools > System

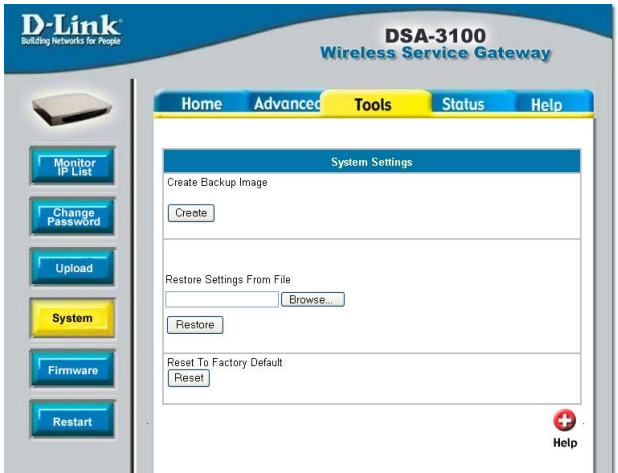
Allows you to make a backup and restore the backup copy to the DSA-3100. This function also enables you to restore the DSA-3100 back to the factory default settings.

Create Backup Image: Make a backup Image file.

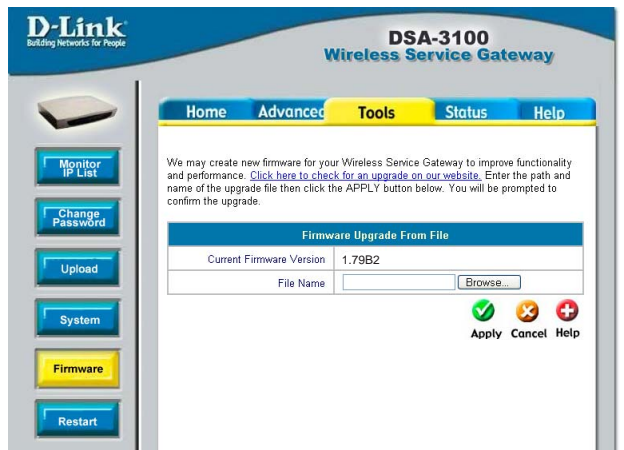
Restore Setting From File: **Browse** the hard drive to restore the backup image file. (Important: The image must be created by the DSA-3100.)

Reset To Factory Default: Click **Reset** to restore the DSA-3100 back to the factory default settings.

Please click the link in the configuration screen shown here to check for firmware upgrades on the D-Link website. After you download the new firmware file to your hard drive, click **Browse** and then click **Apply** to upgrade the firmware.



Tools > Firmware



Caution:

Firmware upgrades might result in configuration data loss. Some other restrictions might also apply. Please refer to the release notes of new firmware upgrades. When the system is upgrading its firmware, the Status LED blinks until done. When finished, the web interface will display a successful message.



Please restart the DSA-3100 using the administration interface. Do not directly power it off and on. Restarting the DSA-3100 in this way after a firmware upgrade might result in corruption of the DSA-3100 firmware. (Online user sessions will be terminated when the system restarts.)

Using the Configuration Utility (continued)

Tools > Restart

Reboots the DSA-3100. It takes about 1 minute for the DSA-3100 to reboot. If you have to turn off the power of the DSA-3100 for some time, please reboot it and remove the power after you hear a beep from it.

Note: On-line user sessions will be terminated when the system restarts.

D-Link Building Networks for People

DSA-3100 Wireless Service Gateway

Home Advanced **Tools** Status Help

Are you sure you want to restart DSA-3100?

Yes Help

Monitor IP List
Change Password
Upload
System
Firmware
Restart

Status > Device Info

This feature displays a system configuration summary. For a chart defining each term, please see the following page.

D-Link Building Networks for People

DSA-3100 Wireless Service Gateway

Home Advanced Tools **Status** Help

System Status	
Current Firmware Version	1.79B2
System Name	DSA-3100
Admin Detail	Management
Succeed Page	http://www.msn.com
External Syslog Server	192.168.0.250:3500
Console Port Baud Rate	9600 bps
Manage	SSH 192.170.0.132
History	Retain Days 3 Days
	Email To cchiu@dlink.com
Time	External Time Server tycho.usno.navy.mil
	Date Time (GMT+0:00) Thu Oct 2 18:58:21 UTC 2003
User	Idle Logout Timer 1000 Min(s)
	Multiple Login Enabled
	User Type RADIUS
	Guest Account Enabled
DNS	Preferred DNS Server 192.152.81.1
	Alternate DNS Server 4.2.2.2

Device Info
Interface
Current Users
Traffic History

Using the Configuration Utility (continued)

Status > Device Info (continued)

Item		Description
Current Firmware Version		The DSA-3100's current firmware version.
System Name		System name; DSA-3100 is the default.
Admin Detail		Information about the admin. If a user encounters a problem connecting to the WAN Port of the DSA-3100, the system admin. information will be shown on the user login page.
Succeed Page		The URL for all users to be directed to after successful login, usually defined as the home page of a corporation.
External Syslog Server		Specify the IP address and Port of the Syslog server.
Console Port baud Rate		Specify the console port's baud rate. The default setting is 9600.
Manage	SSH	The IP address that connects to the WAN Port for configuring the DSA-3100.
	Retain Days	The system will keep login user information for 3 days.
History	E-mail To	E-mail the traffic history file to this address.
	External Time server	The DSA-3100 use this timeserver for clock synchronization.
Time	Date Time (GMT+0:00)	The Date / Time found on this page is Greenwich time (GMT+0:00)
	Idle Logout Timer	If the on-line user is idle for 10 minutes, the session will be ended.
User	Multiple Login	Disable a single user account from logging into the system multiple times.
	User Type	User account authentication method: Local
	Guest Account	Enable guest account.
DNS	Preferred DNS serve	DNS server IP address (Primary).
	Alternate DNS server	DNS server IP address (secondary).

Using the Configuration Utility (continued)

With this feature, you can get Interface management information about the **WAN port**, **Authentication port**, and **Local Network port**. For more detail see the following page:

Status > Interface

WAN	MAC Address	WAN port's MAC address
	IP Address	WAN port's IP address
	Subnet Mask	WAN port's Subnet Mask
	DNS IP Address	WAN port's DNS IP address
Authentication	Mode	Authentication port modes: NAT mode
	MAC Address	Authentication port's MAC address
	IP Address	Authentication port's IP address
	Subnet Mask	Authentication port's Subnet Mask
Authentication DHCP Server	DNS	Authentication port's DNS IP address
	Status	Enable DHCP server on Authentication port
	WINS IP Address	Configure WINS server IP address on DHCP server
	Start IP Address	DHCP pool start IP address
	End IP address	DHCP pool end IP address
Local Network	Lease Time	IP address lease time
	Mode	Local Network port modes: NAT mode
	MAC Address	Local Network port's MAC address
	IP Address	Local Network port's IP address
	Subnet Mask	Local Network port's Subnet Mask
Local Network DHCP Server	DNS IP Address	Local Network port' DNS IP address
	Status	Enable DHCP function on Local Network port.
	WINS IP Address	Configure WINS server IP address on DHCP server
	Start IP Address	DHCP pool start IP address
	End IP address	DHCP pool end IP address
Local Network DHCP Server	Lease Time	IP address lease time

Using the Configuration Utility (continued)

Status > Interface (continued)

Below is an example of the Interface described on the previous page:

Interface Status		
WAN	MAC Address	00:40:05:07:5D:EC
	IP Address	10.2.3.101
	Subnet Mask	255.255.255.0
	DNS IP Address	168.95.1.1
Authentication	Mode	NAT
	MAC Address	00:40:05:07:5D:EE
	IP Address	192.168.1.40
	Subnet Mask	255.255.255.0
Authentication DHCP Server	DNS IP Address	168.95.1.1
	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.101
	End IP Address	192.168.1.200
Local Network	Lease Time	1440 Min(s)
	Mode	NAT
	MAC Address	00:40:05:07:5D:ED
	IP Address	192.168.0.40
	Subnet Mask	255.255.255.0
Local Network DHCP Server	DNS IP Address	168.95.1.1
	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.0.101
	End IP Address	192.168.0.200
	Lease Time	1440 Min(s)

Using the Configuration Utility (continued)

Status > Current Users

With this feature, you could get information about online users including **Username, IP, MAC, packet count, byte count** and **idle time**. It also allows the administrator to force an on-line user to get off-line by clicking the **kick out** link beside a user's data.

The screenshot shows the 'Current Users' page of the D-Link DSA-3100 configuration utility. The page has a navigation menu with 'Home', 'Advanced', 'Tools', 'Status', and 'Help'. The 'Status' tab is selected. On the left, there are buttons for 'Device Info', 'Interface', 'Current Users', and 'Traffic History'. The main content area displays a table with the following columns: No., Username, IP Address, MAC Address, Packets, Bytes, Idle, and Logout. A 'Refresh' button is located below the table. A 'Help' link with a red plus icon is in the bottom right corner.

No.	Username	IP Address	MAC Address	Packets	Bytes	Idle	Logout
-----	----------	------------	-------------	---------	-------	------	--------

Status > Traffic History

This feature gives you access to network access history collected by the DSA-3100. Traffic histories are organized by day. The DSA-3100 will store up to 3 days of history data in its volatile memory.

Note: Since the traffic history is stored in a volatile memory, please copy the log data manually if you need to reboot the DSA-3100 and want to keep the log data.

If you have an e-mail address entered in the system configuration interface, you will have the log sent to that e-mail everyday.

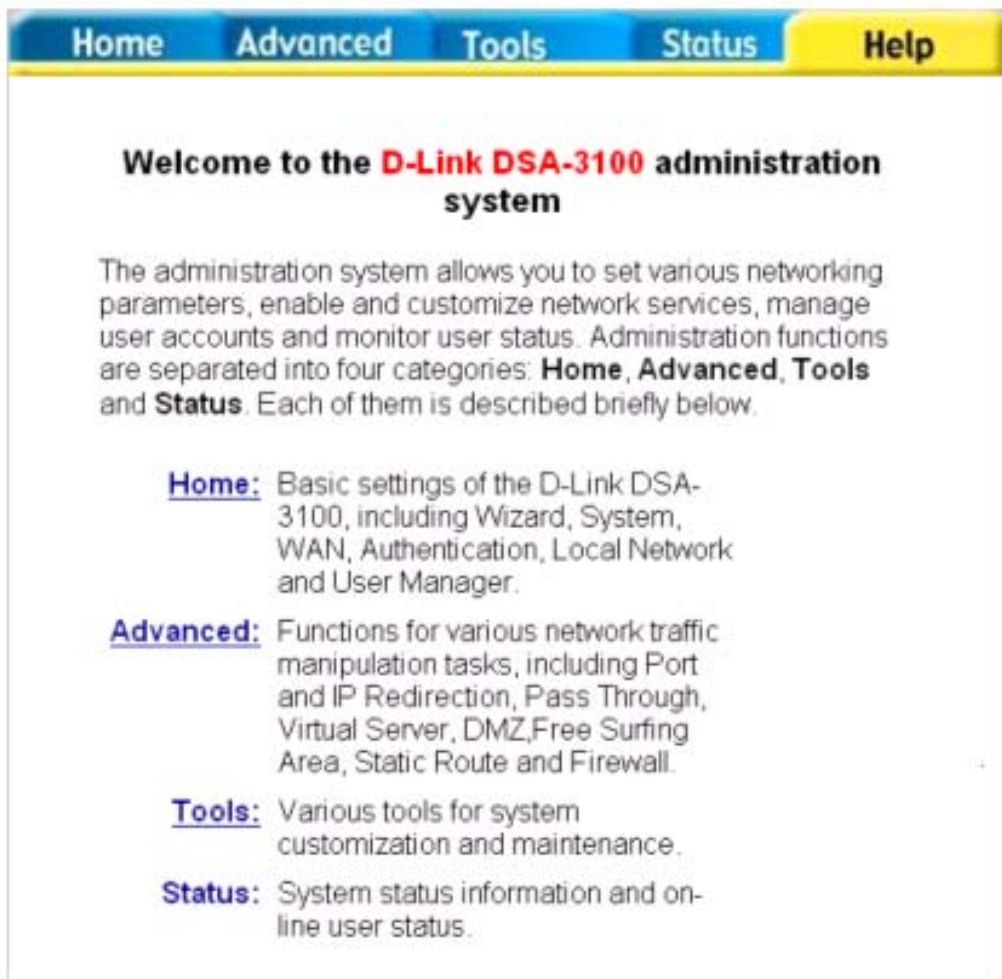
The traffic history is a pure text log. The first line is the header. From line two onward, each line contains a single log record. Each record consists of seven fields. A tab separates each field from the other. This format allows easy import of the log data into other programs for further processing.

The screenshot shows the 'Traffic History' page of the D-Link DSA-3100 configuration utility. The page has a navigation menu with 'Home', 'Advanced', 'Tools', 'Status', and 'Help'. The 'Status' tab is selected. On the left, there are buttons for 'Device Info', 'Interface', 'Current Users', and 'Traffic History'. The main content area displays a table with the following columns: Date and Size. A single log record is shown for the date 2003-10-02 with a size of 37. A 'Help' link with a red plus icon is in the bottom right corner.

Date	Size
2003-10-02	37

Using the Configuration Utility (continued)

Help



Home **Advanced** **Tools** **Status** **Help**

Welcome to the D-Link DSA-3100 administration system

The administration system allows you to set various networking parameters, enable and customize network services, manage user accounts and monitor user status. Administration functions are separated into four categories: **Home**, **Advanced**, **Tools** and **Status**. Each of them is described briefly below.

Home: Basic settings of the D-Link DSA-3100, including Wizard, System, WAN, Authentication, Local Network and User Manager.

Advanced: Functions for various network traffic manipulation tasks, including Port and IP Redirection, Pass Through, Virtual Server, DMZ, Free Surfing Area, Static Route and Firewall.

Tools: Various tools for system customization and maintenance.

Status: System status information and on-line user status.

This feature provides online instructions for operating the DSA-3100, you can click the hyperlink for a more detailed description.

Networking Basics

Using the Network Setup Wizard in Windows XP

In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP**.

Note: Please refer to websites such as <http://www.homenethelp.com> and <http://www.microsoft.com/windows2000> for information about networking computers using Windows 2000, ME or 98.

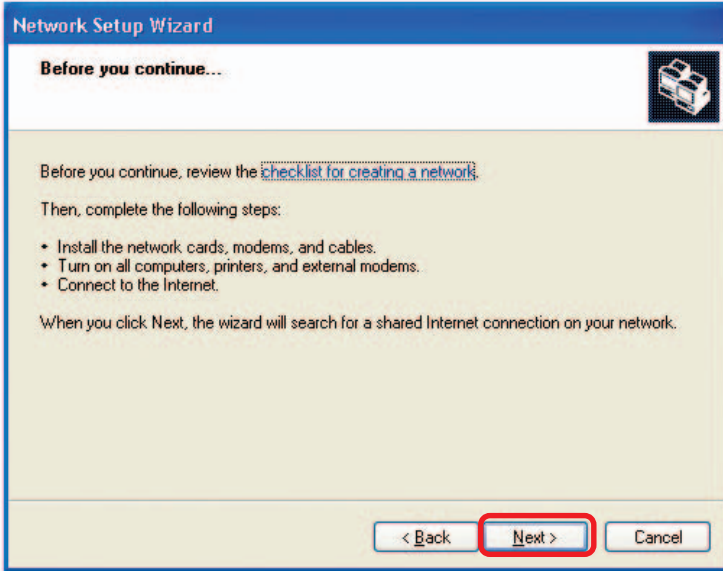
Go to **Start>Control Panel>Network Connections**
Select **Set up a home or small office network**



When this screen appears, click **Next**.

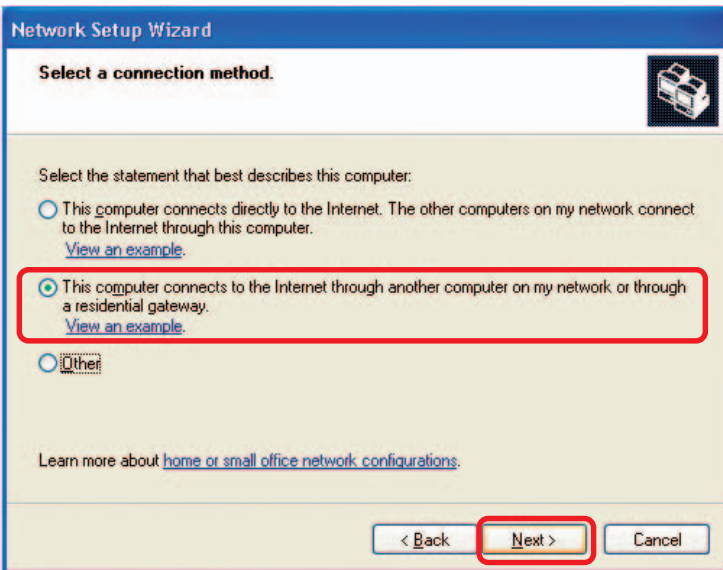
Networking Basics (continued)

Please follow all the instructions in this window:



Click **Next**

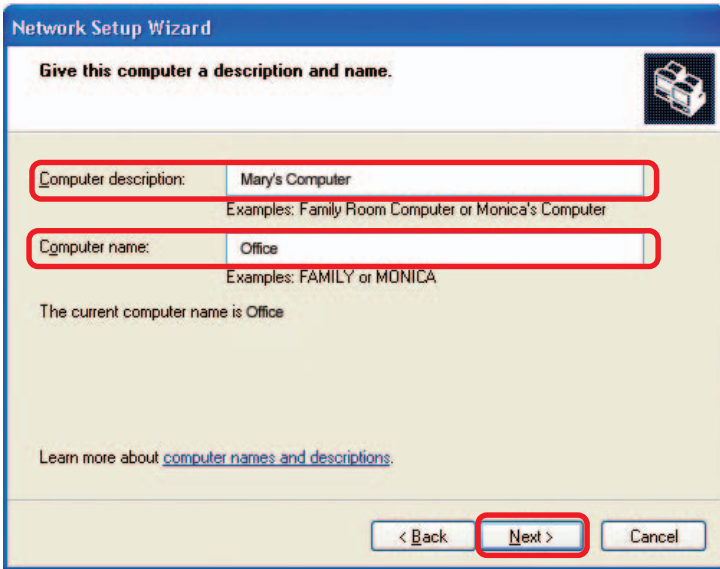
In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.



Click **Next**

Networking Basics (continued)

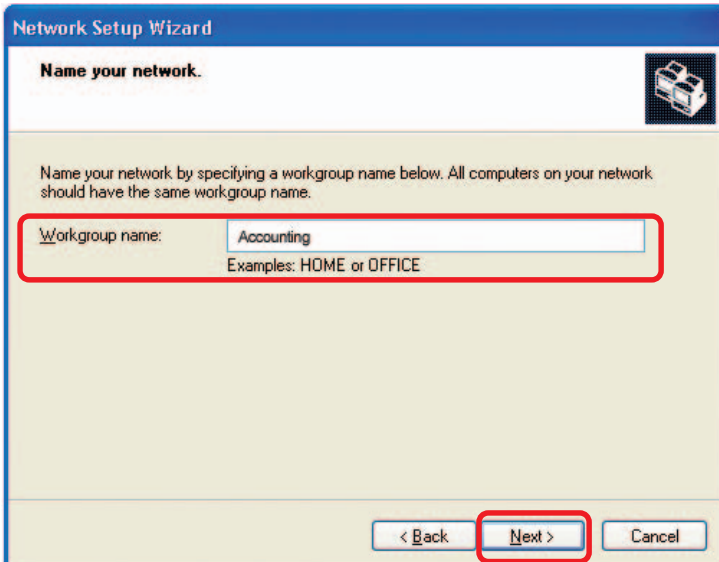
Enter a **Computer description** and a **Computer name** (optional.)



The screenshot shows the 'Network Setup Wizard' window with the title 'Give this computer a description and name.' There are two text input fields: 'Computer description:' containing 'Mary's Computer' and 'Computer name:' containing 'Office'. Both fields are highlighted with a red rectangle. Below the 'Computer name' field, it says 'The current computer name is Office'. At the bottom, the 'Next >' button is highlighted with a red rectangle.

Click **Next**

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup name**.

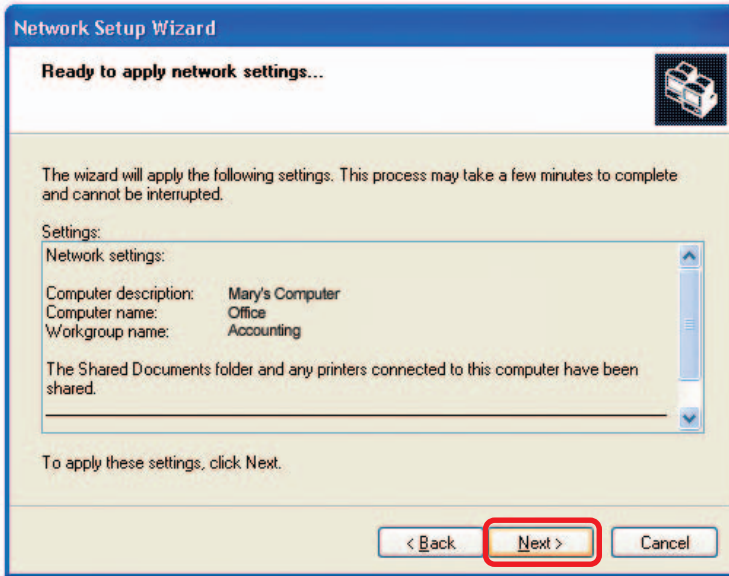


The screenshot shows the 'Network Setup Wizard' window with the title 'Name your network.' There is one text input field: 'Workgroup name:' containing 'Accounting'. This field is highlighted with a red rectangle. At the bottom, the 'Next >' button is highlighted with a red rectangle.

Click **Next**

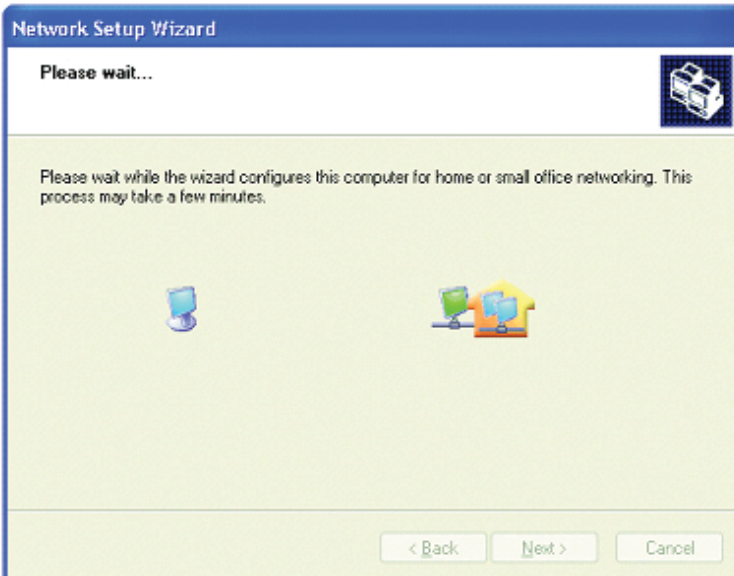
Networking Basics (continued)

Please wait while the **Network Setup Wizard** applies the changes.



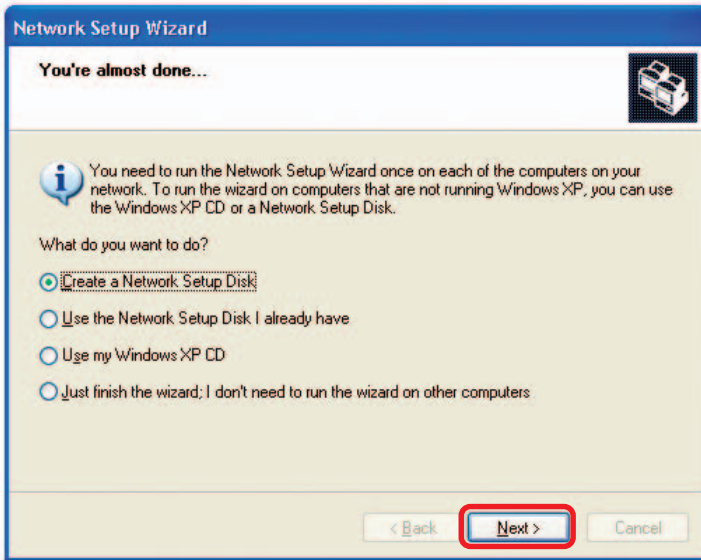
When the changes are complete, Click **Next**.

Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.

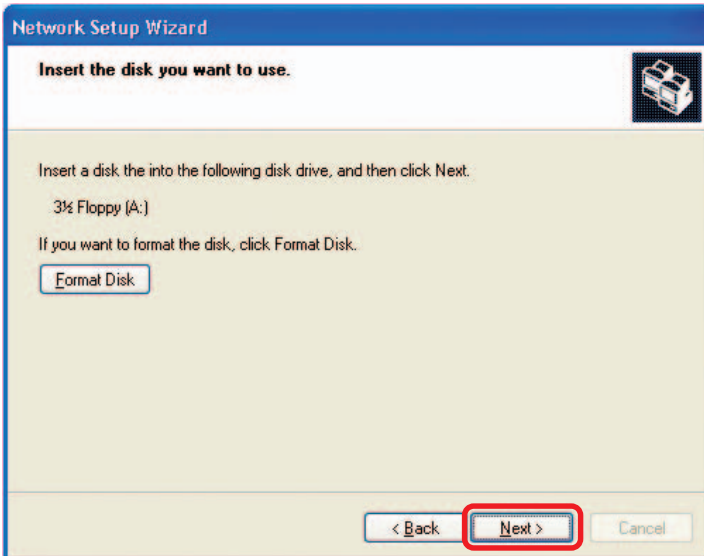


Networking Basics (continued)

In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.

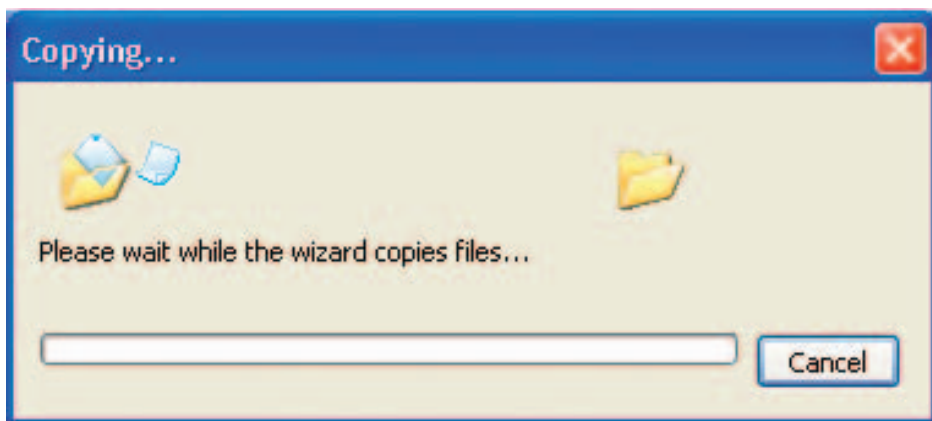


Insert a disk into the Floppy Disk Drive, in this case drive **A**.

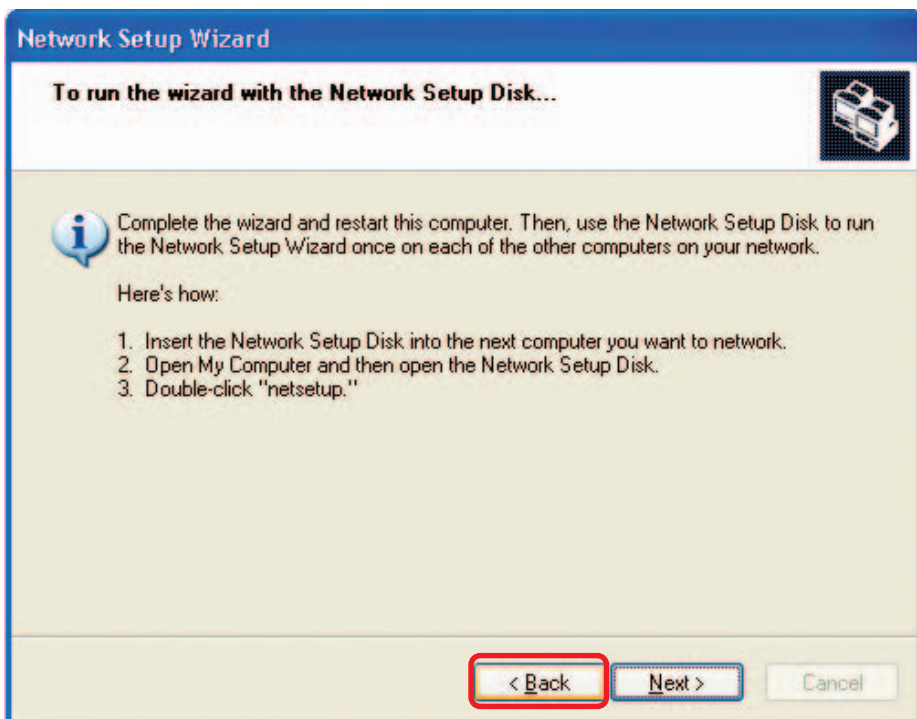


Click **Next**

Networking Basics (continued)



Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. Click **Next**.

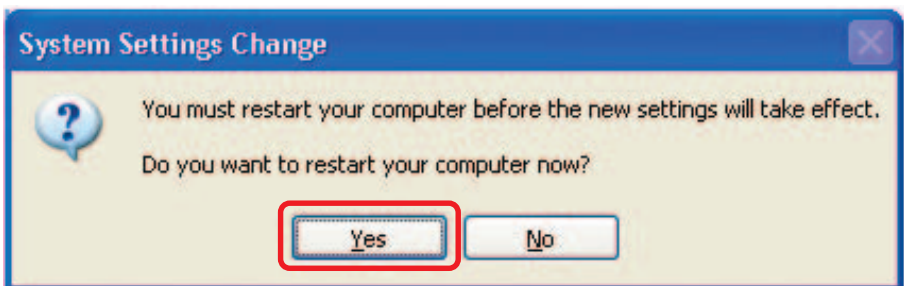


Networking Basics (continued)

Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.



The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.



You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

Networking Basics (continued)

Naming your Computer

To name your computer In **Windows XP**, please follow these directions:

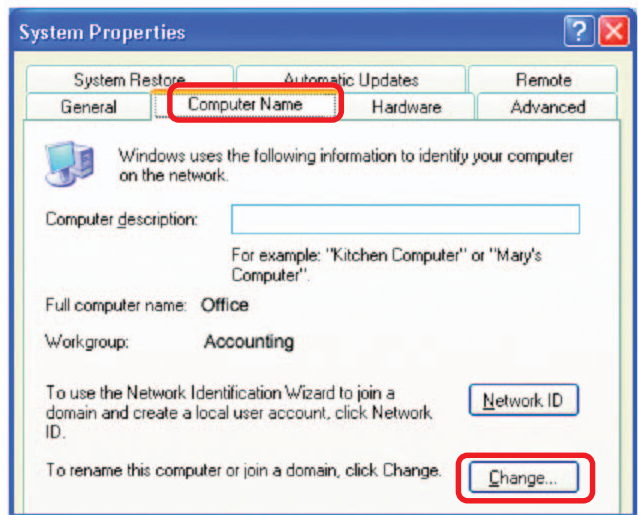
- Click **Start** (in the lower left corner of the screen)
- **Right-click** on **My Computer**
- Select **Properties**



- Select the **Computer Name Tab** in the System Properties window.

- You may enter a **Computer Description** if you wish; this field is optional.

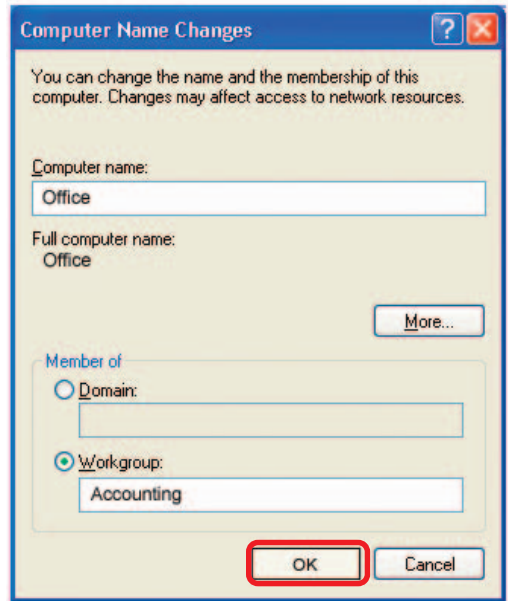
- To rename the computer and join a domain, click **Change**.



Networking Basics (continued)

Naming your Computer (continued)

- In this window, enter the **Computer name**.
- Select **Workgroup** and enter the name of the **Workgroup**.
- All computers on your network must have the same **Workgroup** name.
- Click **OK**



Checking the IP Address in Windows XP

The adapter-equipped computers in your network must be in the same IP Address range (see *Getting Started* in this manual for a definition of IP Address Range.) To check on the IP Address of the adapter, please do the following:

- Right-click on the **Local Area Connection icon** in the task bar
- Click on **Status**



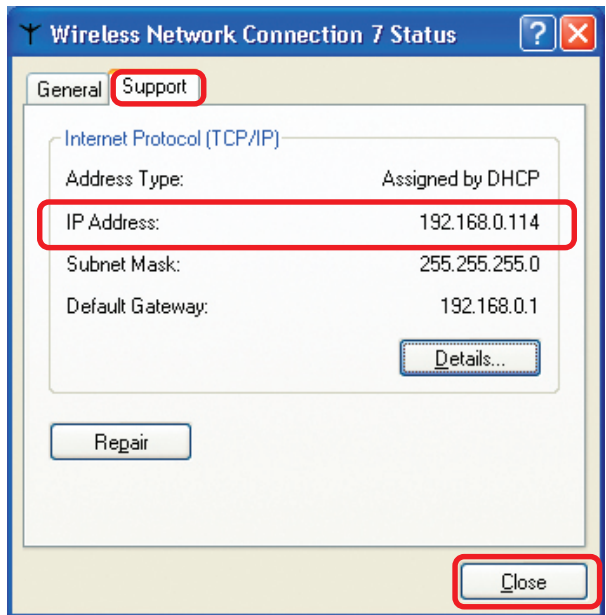
Networking Basics (continued)

Checking the IP Address in Windows XP (continued)

This window will appear.

- Click the **Support** tab

- Click **Close**



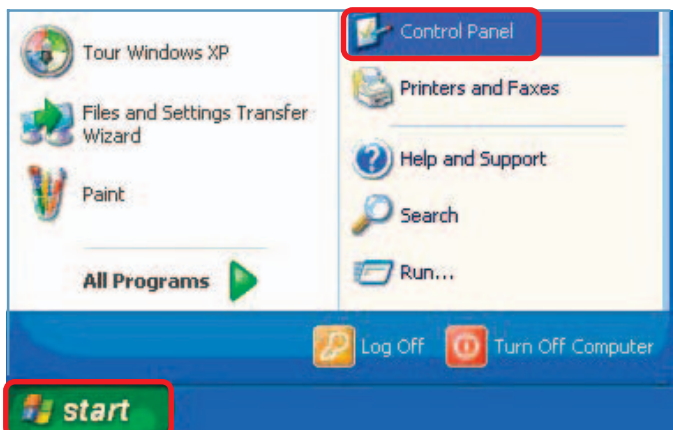
Assigning a Static IP Address in Windows XP/2000

Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

- Go to **Start**

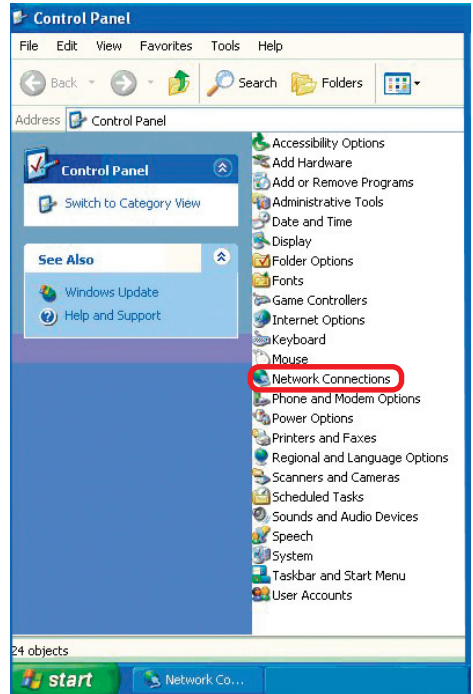
- Double-click on **Control Panel**



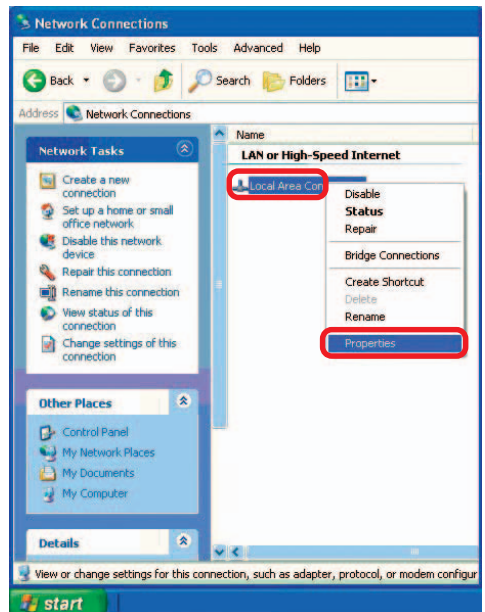
Networking Basics (continued)

Assigning a Static IP Address in Windows XP/2000 (continued)

- Double-click on **Network Connections**



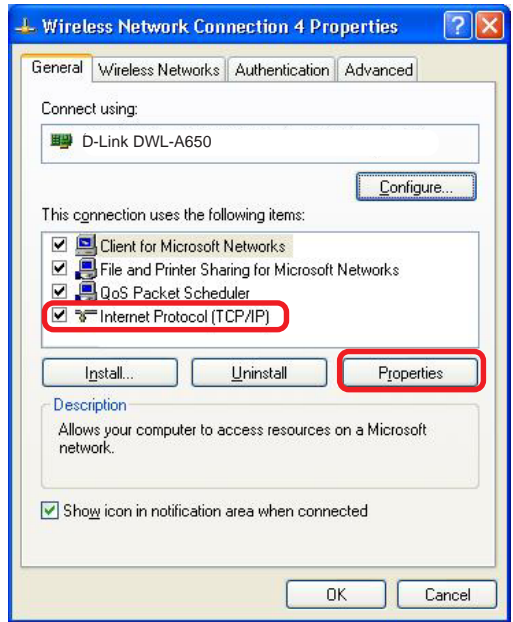
- Right-click on **Local Area Connections**
- Double-click on **Properties**



Networking Basics (continued)

Assigning a Static IP Address in Windows XP/2000

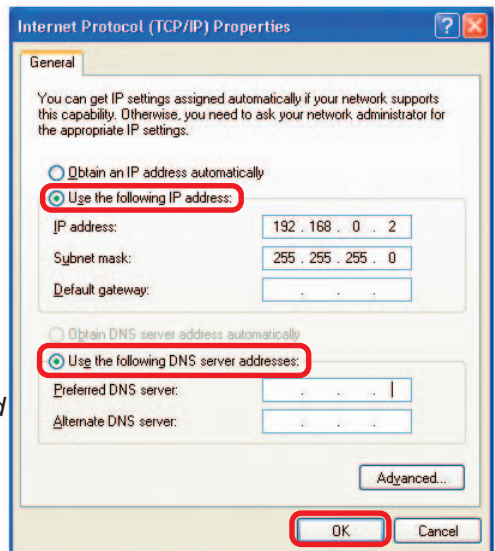
- Click on **Internet Protocol (TCP/IP)**
- Click **Properties**
- Input your **IP Address and subnet mask**. (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)



- Input your **DNS server addresses**. (Note: If you are entering a DNS server, you must enter the IP Address of the Default Gateway.)

The DNS server information will be supplied by your ISP (Internet Service Provider.)

- Click **OK**

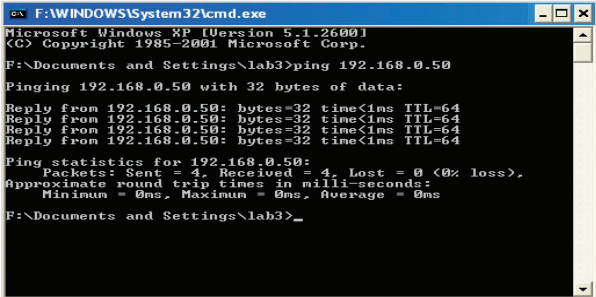


Networking Basics (continued)

Checking the Wireless Connection by Pinging in Windows XP/2000

Note: The following illustrations are examples only. The IP Address that you are pinging may be different from those in the following examples.

- Go to **Start > Run >** type **cmd**. A window similar to this one will appear. Type **ping xxx.xxx.xxx.xxx**, where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the Wireless Router or Access Point, as shown.



```
F:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab3>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

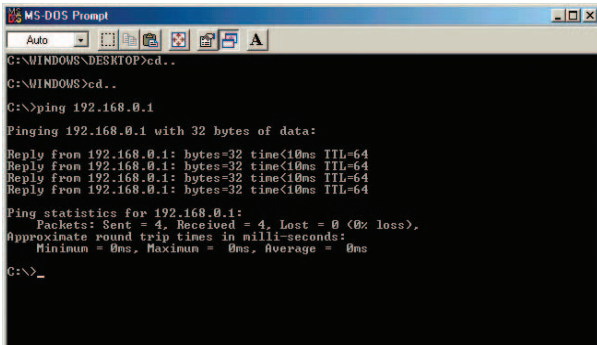
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64
Reply from 192.168.0.50: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

F:\Documents and Settings\lab3>_
```

Checking the Wireless Connection by Pinging in Windows Me/98

- Go to **Start > Run >** type **command**. A window similar to this will appear. Type **ping xxx.xxx.xxx.xxx** where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the wireless router or access point, as shown.



```
MS-DOS Prompt
Auto
C:\WINDOWS\DESKTOP>cd..
C:\WINDOWS>cd..
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<10ms TTL=64
Reply from 192.168.0.1: bytes=32 time<10ms TTL=64
Reply from 192.168.0.1: bytes=32 time<10ms TTL=64
Reply from 192.168.0.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

Technical Specifications

Functions Provided

3 10/100Mbps Fast Ethernet ports for WAN connection, trusted LAN connection and untrusted LAN connection

Manages up to 250 user account data with internal user account database

Supports up to 50 on-line users

ID/Password based authentication and authorization- Can be combined with MAC Address locking to provide stricter access control

POP3, RADIUS and LDAP external authentication mechanism support - Only one of these can be selected at a time

On-line status monitoring and history traffic data review

SSL protected access to the administration interface and user authentication interface

Customizable user login, logout web interface

Customizable target URL for users who successfully get authorization

Built-in DHCP server

High-speed policy routing engine

Customizable preemptory traffic redirection NTP client

Local network port for connecting a trusted network

Permits access to WAN and LAN from local network without authentication

Permits connection to wired Ethernet while connecting the wireless network to this Ethernet port

Technical Specifications (continued)

CPU

NS GX-1 300MHz

Memory

SDRAM 32 MB

Device Ports

WAN port: 10/100Mbps Fast Ethernet

LAN port: 10/100Mbps Fast Ethernet connects to workstations & servers that do not need authentication

LAN port: 10/100Mbps Fast Ethernet connects to workstations & devices that need authentication

Console port: RS-232 (default set to 115200, n, 8, 1, no flow control)

Power Supply

External Power Adapter

Power Input

DC 5V/3A

Power Input

DC 5V/3A

Dimensions

45 mm (H) x 163 mm (D) x 215 mm (W)

Power Input

DC 5V/3A

Dimensions

45mm (H) x 163 mm (D) x 215 mm (W)

Operating Temperature

0° - 50°C

Storage Temperature

-25° - 55°C

EMI Certification

FCC Class A

CE Class A

VCCI Class A

C-Tick

Safety

UL

CSA

TUV/GS

T-Mark

Technical Support

You can find software updates and user documentation on the D-Link Websites

D-Link Provides technical support for customers within the UK.
If you are outside of the UK, please contact your local D-Link Office for technical support

Technical Support within UK

D-Link Technical support over Telephone

DI-ALL & DSL-ALL
(020) 7 365 8440
Mon-Fri 8.00am to 10.00pm

For all other D-Link Products
0845 0800 288
Mon-Fri 9.00am to 6.00pm

D-Link Technical Support over the Internet

<http://www.dlink.co.uk>
<ftp://ftp.dlink.co.uk>
<http://support.dlink.de/solution/sslogin.asp>

D-Link®
Building Networks for People

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>